

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-135944

(43)公開日 平成10年(1998)5月22日

(51) Int.Cl.
 H 04 L 9/18
 G 10 L 9/18
 G 11 B 20/10
 // H 03 M 7/30

識別記号

F I	
H 04 L 9/00	6 5 1
G 10 L 9/18	A
G 11 B 20/10	H
H 03 M 7/30	Z

審査請求 未請求 請求項の数15 O.L (全16頁)

(21)出願番号 特願平8-288542

(22)出願日 平成8年(1996)10月30日

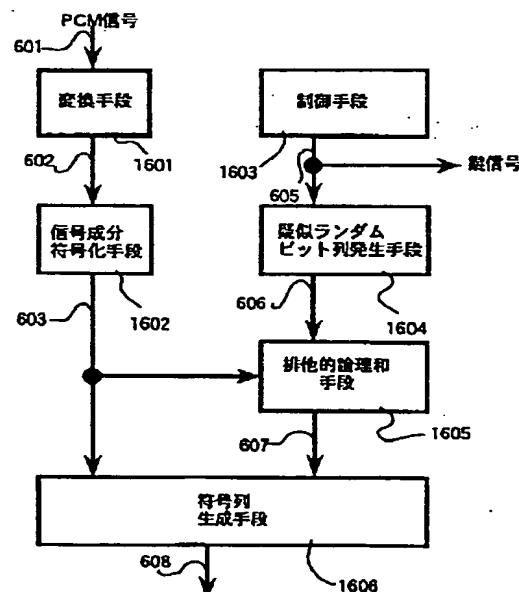
(71)出願人 000002185
 ソニー株式会社
 東京都品川区北品川6丁目7番35号
 (72)発明者 筒井 京弥
 東京都品川区北品川6丁目7番35号 ソニ
 一株式会社内
 (74)代理人 弁理士 小池 晃 (外2名)

(54)【発明の名称】 情報符号化方法、記録媒体、及び復号化装置

(57)【要約】

【課題】 暗号化の鍵情報がなくても情報信号を低品質で再生することを可能とする。

【解決手段】 入力されたPCM信号を変換手段1601で周波数信号成分に変換し、信号成分符号化手段1602で符号化し、高域成分を排他的論理和手段1605に送って疑似ランダムビット列発生手段1604からの疑似ランダムビット列との排他的論理和をとる。符号列生成手段1606では、信号成分符号化手段1602からの低域成分と排他的論理和手段1605からの暗号化された高域成分とを有する符号列1608を生成する。



【特許請求の範囲】

【請求項1】 入力された情報信号を、内容を把握できる低品質の第一の信号成分と、高品質再生のための第二の信号成分とに分割する工程と、

上記第二の信号成分のみを暗号化して符号化する工程とを有することを特徴とする情報符号化方法。

【請求項2】 上記第一の信号成分は上記入力情報信号の低域成分であり、上記第二の信号成分は上記入力情報信号の高域成分であることを特徴とする請求項1記載の情報符号化方法。

【請求項3】 上記符号化は入力信号を圧縮するように符号化するものであることを特徴とする請求項1記載の情報符号化方法。

【請求項4】 一部の情報は低品質再生用の第一の符号と高品質再生用の第二の符号とに二重に符号化され、上記第一の符号は暗号化しないことを特徴とする請求項1記載の情報符号化方法。

【請求項5】 上記信号は音響信号であることを特徴とする請求項1記載の情報符号化方法。

【請求項6】 情報信号が、内容を把握できる低品質の第一の信号成分と、高品質再生のための第二の信号成分とに分割され、上記第二の信号成分のみが暗号化されて符号化されていることを特徴とする記録媒体。

【請求項7】 上記第一の信号成分は上記入力情報信号の低域成分であり、上記第二の信号成分は上記入力情報信号の高域成分であることを特徴とする請求項6記載の記録媒体。

【請求項8】 上記符号化は入力信号を圧縮するように符号化するものであることを特徴とする請求項6記載の記録媒体。

【請求項9】 一部の情報は低品質再生用の第一の符号と高品質再生用の第二の符号とに二重に符号化され、上記第一の符号は暗号化しないことを特徴とする請求項6記載の記録媒体。

【請求項10】 上記信号は音響信号であることを特徴とする請求項6記載の記録媒体。

【請求項11】 情報信号が、内容を把握できる低品質の第一の信号成分と、高品質再生のための第二の信号成分とに分割され、上記第二の信号成分のみが暗号化されて符号化された符号化信号が供給され、上記暗号化の鍵信号の有無によって上記符号化信号の内の上記第二の信号成分を復号化するか否かを選択することを特徴とする復号化装置。

【請求項12】 上記第一の信号成分は上記入力情報信号の低域成分であり、上記第二の信号成分は上記入力情報信号の高域成分であることを特徴とする請求項11記載の復号化装置。

【請求項13】 上記第一の信号成分は上記入力情報信号の低域成分であり、上記第二の信号成分は上記入力情報信号の高域成分であることを特徴とする請求項11記

【特許請求の範囲】

【請求項14】 上記符号化は入力信号を圧縮するように符号化するものであることを特徴とする請求項11記載の復号化装置。

【請求項15】 上記信号は音響信号であることを特徴とする請求項11記載の復号化装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、オーディオPCM信号等の情報信号を暗号化して符号化する情報符号化方法、符号化された信号が記録された記録媒体、及び符号化信号を復号化する復号化装置に関するものである。

【0002】

【従来の技術】 例えば音響信号や映像信号などの情報信号を暗号化して放送したり、記録媒体に記録して、鍵を購入した者に対してのみその視聴を許可する、というソフトの流通方法が知られている。暗号化の方法としては、例えば、PCMの音響信号のビット列に対して鍵信号として乱数系列の初期値を与える、発生した0/1の乱数系列と上記PCMのビット列との排他的論理和をとったビット列を送信したり記録媒体に記録する方法が知られている。この方法を使用することにより、鍵信号入手した者のみがその音響信号を正しく再生できるようにし、鍵信号入手しなかった者は雑音しか再生できないようにすることができる。

【0003】 一方、音響信号を圧縮して放送したり、記録媒体に記録する方法が普及しており、符号化されたオーディオ或いは音声等の信号を記録可能な光磁気ディスク等の記録媒体が広く使用されている。オーディオ或いは音声等の信号の高能率符号化の手法には種々あるが、例えば、時間軸上のオーディオ信号等をブロック化しないで、複数の周波数帯域に分割して符号化する非ブロック化周波数帯域分割方式である、帯域分割符号化（サブ・バンド・コーディング：SBC）や、時間軸の信号を周波数軸上の信号に変換（スペクトル変換）して複数の周波数帯域に分割し、各帯域毎に符号化するブロック化周波数帯域分割方式、いわゆる変換符号化等を挙げることができる。また、上述の帯域分割符号化と変換符号化とを組み合わせた高能率符号化の手法も考えられており、この場合には、例えば、上記帯域分割符号化で帯域分割を行った後、該各帯域毎の信号を周波数軸上の信号にスペクトル変換し、このスペクトル変換された各帯域毎に符号化が施される。

【0004】 ここで、上述したフィルタとしては、例えばQMFフィルタがあり、このQMFフィルタについては、文献「1976, R. E. Crochiere, Digital coding of speech in subbands, Bell Syst. Tech. J. Vol.55, N 0.8 1976」に述べられている。また、文献「ICASSP 83, BOSTON Polyphase Quadrature filters-A new subband coding technique, Joseph H. Rothweiler」には、

等バンド幅のフィルタ分割手法が述べられている。

【0005】ここで、上述したスペクトル変換としては、例えば入力オーディオ信号を所定単位時間（フレーム）でブロック化し、当該ブロック毎に離散フーリエ変換（DFT）、コサイン変換（DCT）、モディファイドDCT変換（MDCT）等を行うことで時間軸を周波数軸に変換するようなスペクトル変換がある。MDCTについては、文献「ICASSP 1987, Subband/Transform Coding Using Filter Bank Designs Based on Time Domain Aliasing Cancellation, J. P. Princen A.B. Bradley, Univ. of Surrey, Royal Melbourne Inst. of Tech.」に述べられている。

【0006】波形信号をスペクトルに変換する方法として上述のDFTやDCTを使用した場合には、M個のサンプルからなる時間ブロックで変換を行うとM個の独立な実数データが得られる。時間ブロック間の接続歪みを軽減するために通常、両隣のブロックとそれぞれM₁個のサンプルずつオーバーラップさせて、平均して、DFTやDCTでは（M-M₁）個のサンプルに対してM個の実数データを量子化して符号化することになる。

【0007】これに対してスペクトルに変換する方法として上述のMDCTを使用した場合には、両隣の時間とN個ずつオーバーラップさせた2M個のサンプルから、独立なM個の実数データが得られるので平均して、MDCTではM個のサンプルに対してM個の実数データを量子化して符号化することになる。復号化装置においては、このようにしてMDCTを用いて得られた符号から各ブロックにおいて逆変換を施して得られた波形要素を互いに干渉させながら加え合わせることにより、波形信号を再構成することができる。

【0008】一般に変換のための時間ブロックを長くすることによって、スペクトルの周波数分解能が高まり特定のスペクトル成分にエネルギーが集中する。したがって、両隣のブロックと半分ずつオーバーラップさせて長いブロック長で変換を行い、しかも得られたスペクトル信号の個数が、元の時間サンプルの個数に対して増加しないMDCTを使用することにより、DFTやDCTを使用した場合よりも効率の良い符号化を行うことが可能となる。また、隣接するブロック同士に十分長いオーバーラップを持たせることによって、波形信号のブロック間歪みを軽減することもできる。

【0009】このようにフィルタやスペクトル変換によって帯域毎に分割された信号を量子化することにより、量子化雑音が発生する帯域を制御することができ、マスキング効果などの性質を利用して聴覚的により高能率な符号化を行なうことができる。また、ここで量子化を行なう前に、各帯域毎に、例えばその帯域における信号成分の絶対値の最大値で正規化を行なうようにすれば、さらに高能率な符号化を行なうことができる。

【0010】周波数帯域分割された各周波数成分を量子

化する周波数分割幅としては、例えば人間の聴覚特性を考慮した帯域分割が行われる。すなわち、一般に臨界帯域（クリティカルバンド）と呼ばれている高域程帯域幅が広くなるような帯域幅で、オーディオ信号を複数（例えば25バンド）の帯域に分割することがある。また、この時の各帯域毎のデータを符号化する際には、各帯域毎に所定のピット配分或いは、各帯域毎に適応的なピット割当て（ピットアロケーション）による符号化が行われる。例えば、上記MDCT処理されて得られた係数データを上記ピットアロケーションによって符号化する際には、上記各ブロック毎のMDCT処理により得られる各帯域毎のMDCT係数データに対して、適応的な割当てピット数で符号化が行われることになる。

【0011】このようなピット割当の手法としては、文献「Adaptive Transform Coding of Speech Signals, R. Zelinski and P. Noll」、及び文献「IEEE Transactions on Acoustics, Speech, and Signal Processing, v. vol. ASSP-25, No.4, August 1977」に記載されている2つの手法が知られている。

20 【0012】これらの文献に記載された技術においては、各帯域毎の信号の大きさをもとに、ピット割当を行なっている。この方式では、量子化雑音スペクトルが平坦となり、雑音エネルギー最小となるが、聴覚的にはマスキング効果が利用されていないために実際の雑音感は最適ではない。

【0013】また、文献「ICASSP 1980, The critical band coder—digital encoding of the perceptual requirements of the auditory system, M. A. Kransner, MIT」では、聴覚マスキングを利用することで、各帯域毎に必要な信号対雑音比を得て固定的なピット割当を行なう手法が述べられている。しかしこの手法ではサイン波入力で特性を測定する場合でも、ピット割当が固定的であるために特性値が、それほど良い値とならない。

【0014】これらの問題を解決するために、ピット割当に使用できる全ピットが、各小ブロック毎にあらかじめ定められた固定ピット割当パターン分と、各ブロックの信号の大きさに依存したピット配分を行なう分に分割使用され、その分割比を入力信号に関係する信号に依存させ、前記信号のスペクトルが滑らかなほど前記固定ピット割当パターン分への分割比率を大きくする高能率符号化装置が提案されている。

【0015】この方法によれば、サイン波入力のように、特定のスペクトルにエネルギーが集中する場合にはそのスペクトルを含むブロックに多くのピットを割り当てる事により、全体の信号対雑音特性を著しく改善することができる。一般に、急峻なスペクトル成分をもつ信号に対して人間の聴覚は極めて敏感であるため、このような方法を用いる事により、信号対雑音特性を改善することは、単に測定上の数値を向上させるばかりでなく、聴感上、音質を改善するのに有効である。

【0016】ピット割り当ての方法にはこの他にも数多くのやり方が提案されており、さらに聴覚に関するモデルが精緻化され、符号化装置の能力があがれば聴覚的にみてより高能率な符号化が可能になる。これらの方法においては、計算によって求められた信号対雑音特性をなるべく忠実に実現するような実数のピット割り当て基準値を求め、それを近似する整数値を割り当てピット数とすることが一般的である。

【0017】また、本件発明者等が先に提案した特願平7-500482号の出願の明細書及び図面においては、スペクトル信号から聴感上特に重要なトーン性の成分、すなわち特定の周波数周辺にエネルギーが集中している信号成分、を分離して、他のスペクトル成分とは別に符号化する方法が開示されており、これにより、オーディオ信号等を聴感上の劣化を殆ど生じさせずに高い圧縮率で効率的に符号化することが可能になっている。

【0018】実際の符号列を構成するにあたっては、まず、正規化および量子化が行なわれる帯域毎に量子化精度情報、正規化係数情報を所定のピット数で符号化し、次に、正規化および量子化されたスペクトル信号を符号化すれば良い。

【0019】また、いわゆるMPEG規格のISO/IEC 11172-3:1993(E), a993においては、帯域によって量子化精度情報を表すビット数が異なるように設定された高能率符号化方式が記述されており、高域になるにしたがって、量子化精度情報を表すビット数が小さくなるように規格化されている。

【0020】さらに、量子化精度情報を直接符号化するかわりに、復号化装置において、例えば、正規化係数情報から量子化精度情報を決定する方法も知られているが、この方法では、規格を設定した時点で正規化係数情報と量子化精度情報の関係が決まってしまうので、将来的にさらに高度な聴覚モデルに基づいた量子化精度の制御を導入することができなくなる。また、実現する圧縮率に幅がある場合には圧縮率毎に正規化係数情報と量子化精度情報との関係を定める必要が出てくる。

【0021】次に、量子化されたスペクトル信号を、例えば、文献「D. A. Huffman: A Method for Construction of Minimum Redundancy Codes, Proc.I.R.E., 40, p. 1098(1952)」に述べられている可変長符号を用いて符号化することによって、より効率的に符号化する方法も知られている。

【0022】上述のように符号化された信号をPCM信号の場合と同様に暗号化して配布することも可能で、この場合、鍵信号入手していない者は元の信号を再生することはできない。また、符号化されたピット列を暗号化するのではなく、PCM信号をランダム信号に変換した後、圧縮のための符号化を行なう方法もあり、この場合も鍵信号入手していない者は雑音しか再生することはできない。

【0023】

【発明が解決しようとする課題】しかしながら、これらのスクランブル方法では、鍵が無い場合、あるいは通常の再生手段で再生させた場合には、それを再生させると雑音になってしまい、そのソフトの内容把握をすることはできない。このため、例えば、比較的低音質で音楽を記録したディスクを配布し、それを試聴した者が自分の気に入ったものに対してだけ鍵を購入して高音質で再生できるようにする、あるいはそのソフトを試聴してから高音質で記録されたディスクを新たに購入できるようにする、といった用途に利用することができなかった。

【0024】また従来、高能率符号化を施した信号を暗号化する場合に、通常の再生手段にとって意味のある符号列を与えるながら、その圧縮効率を下げないようにすることは困難であった。すなわち、前述のように、高能率符号化を施してできた符号列にスクランブルをかけた場合、その符号列を再生しても雑音が発生するばかりではなく、スクランブルによってできた符号列が、元の高能率符号の規格に適合していない場合には、再生手段がまったく動作しないこともありうる。

【0025】また逆に、PCM信号にスクランブルをかけた後、高能率符号化した場合には例えば聴覚の性質を利用して情報量を削っていると、その高能率符号化を解除した時点で、必ずしも、PCM信号にスクランブルをかけた信号が再現できるわけでは無いので、スクランブルを正しく解除することは困難なものになってしまう。このため、圧縮の方法としては効率は下がっても、スクランブルが正しく解除できる方法を選択する必要があった。

【0026】本発明はこのような実情を鑑みてなされたものであり、オーディオ信号やビデオ信号等の情報信号を暗号化して伝送したり記録媒体に記録して供給する場合に、暗号化の鍵が無くとも内容が確認できる程度の低品質の再生が行え、鍵を用いることによってより品質の高い再生が行えるような情報符号化方法、記録媒体、及び復号化装置を提供することを目的とするものである。

【0027】

【課題を解決するための手段】本発明に係る情報符号化方法は、上述した課題を解決するために、入力された情報信号を、内容を把握できる程度の低い品質の第一の信号成分と、高品質再生のための第二の信号成分とに分割し、上記第二の信号成分のみを暗号化して符号化することを特徴としている。

【0028】すなわち、信号を比較的低い品質ではあるが内容を十分把握することができる第一の信号成分と高品質再生のための第二の信号成分に分け、そのうちの第一の信号成分は、スクランブル等の暗号化の解除機能の無い再生手段でも再生できるようにするとともに、それを解読するための鍵を受け取った再生手段では第二の信号成分も含めて再生できるようにすることによって高品

質再生を可能にするものである。

【0029】本発明は、このような符号化が施された信号を記録して成る記録媒体に適用できる。

【0030】本発明に係る復号化装置は、情報信号が、内容を把握できる低品質の第一の信号成分と、高品質再生のための第二の信号成分とに分割され、上記第二の信号成分のみが暗号化されて符号化された符号化信号が供給され、上記暗号化の鍵信号の有無によって上記符号化信号の内の上記第二の信号成分を復号化するか否かを選択することを特徴としている。

【0031】ここで、上記符号化は入力信号を圧縮するように符号化するものであることが挙げられる。また、一部の情報は低品質再生用の第一の符号と高品質再生用の第二の符号とに二重に符号化され、上記第一の符号は暗号化しないことが挙げられる。この一部の情報としては、上記第二の信号成分に関する情報が挙げられる。さらに、上記信号は音響信号であることが挙げられる。

【0032】また、本発明は、信号を高能率符号化してから暗号化をかけるが、そのようにしてできた符号列が鍵の無い再生手段にとって意味のある符号列によって、広い範囲の再生装置で比較的低品質の再生を可能にするものである。

【0033】

【発明の実施の形態】以下、本発明に係る情報符号化方法、記録媒体、及び復号化装置の好ましい実施の形態について、図面を参照しながら説明する。

【0034】先ず、本発明に用いられる暗号化の技術について、図1乃至図3を参照しながら説明する。

【0035】図1は、暗号化したビット列を生成するための暗号化装置の構成例を示すブロック図である。この暗号化装置では、入力情報信号であるPCM信号703の各ビットを排他的論理和手段1703に送り、制御手段1701から送られた初期値情報701を利用して発生された、疑似ランダムビット列発生手段1702の出力702との排他的論理和をとることにより、ビット列704を出力する。疑似ランダムビット列発生手段1702としては、例えば、長さが100ビットの任意に選択したビット列を初期値として、それを自乗して中央の100ビットのみを残すという操作を繰り返して得られる乱数列の下から50番めのビットを選択するようにして構成することができる。このようにして、出力されたビット列を例えば光ディスクに記録することによって、正しい鍵（この場合は、初期値情報701）入手したもののみ、元のPCM信号を再生できるようにすることができます。

【0036】図2は、図1の暗号化装置が output したビット列704を復号化するための復号化装置の構成例を示したものである。疑似ランダムビット列発生手段1802は図1の疑似ランダムビット列発生手段1702と同じ機能を持ち、したがって、同じ鍵信号が初期値として

与えられれば、同じ疑似ランダムビット列が得られる。この疑似ランダムビット列803と入力信号804は排他的論理和がとられる。ここで図3に示すように、ビットAに対して二度、ビットBとの排他的論理和をとると、ビットAが再現されるので、正しい鍵信号が入手されている場合にはビット列805を正しく再生することができる。図2の例では、鍵情報801が制御手段1801に供給され、制御手段1801は上記図1の制御手段1701からの初期値情報701に等しい初期値情報

10 802を疑似ランダムビット列発生手段1802に送ることで、図1の暗号化のときと同じ疑似ランダムビット列を疑似ランダムビット列発生手段1802に発生させて排他的論理和手段1803に送っている。

【0037】しかしながら、入力情報信号であるPCM信号に対して全体的に上述したような暗号化を施した場合には、正しい鍵信号を入手しないと、ディスク等の媒体に記録されているソフトの内容をまったく知ることができないので、ディスクを入手した者がそれを解読するための鍵信号を購入すべきかどうかの判断をすることが困難であった。このため、例えば安い価格でソフトを配布し、それを試聴したユーザーが気に入ったものに対してのみ鍵信号を購入するといったことはできなかった。

【0038】そこで、このような問題を解決するため、本発明の実施の形態においては、入力情報信号であるPCM信号を二つの信号成分に分割し、一方のみを暗号化して符号化している。これらの二つの信号成分については、入力されたPCM信号の低域成分を第一の信号成分とし、高域成分を第二の信号成分として、第二の信号成分のみを暗号化することが挙げられる。

30 【0039】ここで、本発明の好ましい実施の形態が適用される圧縮データ記録及び／又は再生装置の一例について、図4を参照しながら説明する。

【0040】図4に示す圧縮データ記録及び／又は再生装置において、記録媒体としては、スピンドルモータ51により回転駆動される光磁気ディスク1を用いている。光磁気ディスク1に対するデータの記録時には、例えば光学ヘッド53によりレーザ光を照射した状態で記録データに応じた変調磁界を磁気ヘッド54により印加することによって、いわゆる磁界変調記録を行い、光磁気ディスク1の記録トラックに沿ってデータを記録する。また再生時には、光磁気ディスク1の記録トラックを光学ヘッド53によりレーザ光でトレースして磁気光学的に再生を行う。

【0041】光学ヘッド53は、例えば、レーザダイオード等のレーザ光源、コリメータレンズ、対物レンズ、偏光ビームスプリッタ、シリンドリカルレンズ等の光学部品及び所定パターンの受光部を有するフォトディクタ等から構成されている。この光学ヘッド53は、光磁気ディスク1を介して上記磁気ヘッド54と対向する位置に設けられている。光磁気ディスク1にデータを記録

するときには、後述する記録系のヘッド駆動回路66により磁気ヘッド54を駆動して記録データに応じた変調磁界を印加すると共に、光学ヘッド53により光磁気ディスク1の目的トラックにレーザ光を照射することによって、磁界変調方式により熱磁気記録を行う。またこの光学ヘッド53は、目的トラックに照射したレーザ光の反射光を検出し、例えればいわゆる非点収差法によりフォーカスエラーを検出し、例えればいわゆるブツシユブル法によりトッキングエラーを検出する。光磁気ディスク1からデータを再生するとき、光学ヘッド53は上記フォーカスエラーやトッキングエラーを検出すると同時に、レーザ光の目的トラックからの反射光の偏光角（カ一回転角）の違いを検出して再生信号を生成する。

【0042】光学ヘッド53の出力は、R.F.回路55に供給される。このR.F.回路55は、光学ヘッド53の出力から上記フォーカスエラー信号やトッキングエラー信号を抽出してサーボ制御回路56に供給するとともに、再生信号を2値化して後述する再生系のデコーダ71に供給する。

【0043】サーボ制御回路56は、例えればいわゆるフォーカスサーボ制御回路やトッキングサーボ制御回路、スピンドルモータサーボ制御回路、スレッドサーボ制御回路等から構成される。上記フォーカスサーボ制御回路は、上記フォーカスエラー信号がゼロになるように、光学ヘッド53の光学系のフォーカス制御を行う。また上記トッキングサーボ制御回路は、上記トッキングエラー信号がゼロになるように光学ヘッド53の光学系のトッキング制御を行う。さらに上記スピンドルモータサーボ制御回路は、光磁気ディスク1を所定の回転速度（例えれば一定線速度）で回転駆動するようにスピンドルモータ51を制御する。また、上記スレッドサーボ制御回路は、システムコントローラ57により指定される光磁気ディスク1の目的トラック位置に光学ヘッド53及び磁気ヘッド54を移動させる。このような各種制御動作を行うサーボ制御回路56は、該サーボ制御回路56により制御される各部の動作状態を示す情報をシステムコントローラ57に送る。

【0044】システムコントローラ57にはキー入力操作部58や表示部59が接続されている。このシステムコントローラ57は、キー入力操作部58による操作入力情報により操作入力情報により記録系及び再生系の制御を行う。またシステムコントローラ57は、光磁気ディスク1の記録トラックからヘッダタイムやサブコードのQデータ等により再生されるセクタ単位のアドレス情報に基づいて、光学ヘッド53及び磁気ヘッド54がトレースしている上記記録トラック上の記録位置や再生位置を管理する。さらにシステムコントローラ57は、本圧縮データ記録再生装置のデータ圧縮率と上記記録トラック上の再生位置情報に基づいて表示部59に再生時間を表示させる制御を行う。

【0045】この再生時間表示は、光磁気ディスク1の記録トラックからいわゆるヘッダタイムやいわゆるサブコードQデータ等により再生されるセクタ単位のアドレス情報（絶対時間情報）に対し、データ圧縮率の逆数（例えば1/4圧縮のときには4）を乗算することにより、実際の時間情報を求め、これを表示部59に表示させるものである。なお、記録時においても、例えればいわゆる光磁気ディスク等の記録トラックに予め絶対時間情報が記録されている（プリフォーマットされている）場合に、このプリフォーマットされた絶対時間情報を読み取ってデータ圧縮率の逆数を乗算することにより、現在位置を実際の記録時間で表示させることも可能である。

【0046】次に、この図4に示すディスク記録／再生装置の記録系において、入力端子60からのアナログオーディオ入力信号A₁₁がローパスフィルタ61を介してA/D変換器62に供給され、このA/D変換器62は上記アナログオーディオ入力信号A₁₁を量子化する。A/D変換器62から得られたデジタルオーディオ信号は、ATC（適応変換符号化：Adaptive Transform Coding）エンコーダ63に供給される。また、入力端子67からのデジタルオーディオ入力信号D₁₁がデジタル入力インターフェース回路68を介してATCエンコーダ63に供給される。ATCエンコーダ63は、上記入力信号A₁₁を上記A/D変換器62により量子化した所定転送速度のデジタルオーディオPCMデータについて、所定のデータ圧縮率に応じたビット圧縮（データ圧縮）処理を行うものであり、ATCエンコーダ63から出力される圧縮データ（ATCデータ）は、メモリ64に供給される。例えればデータ圧縮率が1/8の場合について

説明すると、ここでデータ転送速度は、標準的なディジタルオーディオCDのフォーマットであるいわゆるCD-Digital Audio Data（データ転送速度（75セクタ/秒）の1/8（9,375セクタ/秒）に低減されている。

【0047】次にメモリ（RAM）64は、データの書き込み及び読み出しがシステムコントローラ57により制御され、ATCエンコーダ63から供給されるATCデータを一時的に記憶しておき、必要に応じてディスク上に記録するためのバッファメモリとして用いられている。すなわち、例えればデータ圧縮率が1/8の場合において、ATCエンコーダ63から供給される圧縮オーディオデータは、そのデータ転送速度が、標準的なCD-Digital Audio Dataのデータ転送速度（75セクタ/秒）の1/8、すなわち9,375セクタ/秒に低減されており、この圧縮データがメモリ64に連続的に書き込まれる。この圧縮データ（ATCデータ）は、前述したように8セクタにつき1セクタの記録を行えば足りるが、このような8セクタおきの記録は事実上不可能に近いため、後述するようなセクタ連続の記録を行うようにしている。

【0048】この記録は、休止期間を介して、所定の複数セクタ（例えば32セクタ+数セクタ）から成るクラスタを記録単位として、標準的なCD-DAフォーマットと同じデータ転送速度（75セクタ/秒）でバースト的に行われる。すなわちメモリ64においては、上記ピット圧縮レートに応じた9.375（=75/8）セクタ/秒の低い転送速度で連続的に書き込まれたデータ圧縮率1/8のATCオーディオデータが、記録データとして上記75セクタ/秒の転送速度でバースト的に読み出される。この読み出されて記録されるデータについて、記録休止期間を含む全体的なデータ転送速度は、上記9.375セクタ/秒の低い速度となっているが、バースト的に行われる記録動作の時間内での瞬時のデータ転送速度は上記標準的な75セクタ/秒となっている。従って、ディスク回転速度が標準的なCD-DAフォーマットと同じ速度（一定線速度）のとき、該CD-DAフォーマットと同じ記録密度、記憶パターンの記録が行われることになる。

【0049】メモリ64から上記75セクタ/秒の（瞬時の）転送速度でバースト的に読み出されたATCオーディオデータすなわち記録データは、エンコーダ65に供給される。ここで、メモリ64からエンコーダ65に供給されるデータ列において、1回の記録で連続記録される単位は、複数セクタ（例えば32セクタ）から成るクラスタ及び該クラスタの前後位置に配されたクラスタ接続用の数セクタとしている。このクラスタ接続用セクタは、エンコーダ65でのインターリーブ長より長く設定しており、インターリーブされても他のクラスタのデータに影響を与えないようにしている。

【0050】エンコーダ65は、メモリ64から上述したようにバースト的に供給される記録データについて、エラー訂正のための符号化処理（パリティ付加及びインターリーブ処理）やEFM符号化処理などを施す。このエンコーダ65による符号化処理の施された記録データが磁気ヘッド駆動回路66に供給される。この磁気ヘッド駆動回路66は、磁気ヘッド54が接続されており、上記記録データに応じた変調磁界を光磁気ディスク1に印加するように磁気ヘッド54を駆動する。

【0051】また、システムコントローラ57は、メモリ64に対する上述の如きメモリ制御を行うとともに、このメモリ制御によりメモリ64からバースト的に読み出される上記記録データを光磁気ディスク1の記録トラックに連続的に記録するように記録位置の制御を行う。この記録位置の制御は、システムコントローラ57によりメモリ64からバースト的に読み出される上記記録データの記録位置を管理して、光磁気ディスク1の記録トラック上の記録位置を指定する制御信号をサーボ制御回路56に供給することによって行われる。

【0052】次に、図4に示すディスク記録／再生装置の再生系について説明する。この再生系は、上述の記録

系により光磁気ディスク1の記録トラック上に連続的に記録された記録データを再生するためのものであり、光学ヘッド53によって光磁気ディスク1の記録トラックをレーザ光でトレスすることにより得られる再生出力がRF回路55により2値化されて供給されるデコーダ71を備えている。この時光磁気ディスクのみではなく、いわゆるCD（コンパクトディスク：Compact Disc）と同じ再生専用光ディスクの読みだしも行なうことができる。

【0053】デコーダ71は、上述の記録系におけるエンコーダ65に対応するものであって、RF回路55により2値化された再生出力について、エラー訂正のための上述の如き復号化処理やEFM復号化処理などの処理を行い、上述のデータ圧縮率1/8のATCオーディオデータを、正規の転送速度よりも早い75セクタ/秒の転送速度で再生する。このデコーダ71により得られる再生データは、メモリ72に供給される。

【0054】メモリ(RAM)72は、データの書き込み及び読み出しがシステムコントローラ57により制御され、デコーダ71から75セクタ/秒の転送速度で供給される再生データがその75セクタ/秒の転送速度でバースト的に書き込まれる。また、このメモリ72は、上記75セクタ/秒の転送速度でバースト的に書き込まれた上記再生データがデータ圧縮率1/8に対応する9.375セクタ/秒の転送速度で連続的に読み出される。

【0055】システムコントローラ57は、再生データをメモリ72に75セクタ/秒の転送速度で書き込むとともに、メモリ72から上記再生データを上記9.375セクタ/秒の転送速度で連続的に読み出すようなメモリ制御を行う。また、システムコントローラ57は、メモリ72に対する上述の如きメモリ制御を行うとともに、このメモリ制御によりメモリ72からバースト的に書き込まれる上記再生データを光磁気ディスク1の記録トラックから連続的に再生するよう再位置の制御を行う。この再位置の制御は、システムコントローラ57によりメモリ72からバースト的に読み出される上記再生データの再位置を管理して、光磁気ディスク1もしくは光ディスク1の記録トラック上の再位置を指定する制御信号をサーボ制御回路56に供給することによって行われる。

【0056】メモリ72から9.375セクタ/秒の転送速度で連続的に読み出された再生データとして得られるATCオーディオデータは、ATCデコーダ73に供給される。このATCデコーダ73は、上記記録系のATCエンコーダ63に対応するもので、例えばATCデータを8倍にデータ伸張（ピット伸張）することで16ビットのデジタルオーディオデータを再生する。このATCデコーダ73からのデジタルオーディオデータは、D/A変換器74に供給される。

【0057】D/A変換器74は、ATCデコーダ73から供給されるデジタルオーディオデータをアナログ信号に変換して、アナログオーディオ出力信号A...を形成する。このD/A変換器74により得られるアナログオーディオ信号A...は、ローパスフィルタ75を介して出力端子76から出力される。

【0058】次に高能率圧縮符号化について詳述する。すなわち、オーディオPCM信号等の入力デジタル信号を、帯域分割符号化(SBC)、適応変換符号化(ATC: Adaptive Transform Coding)及び適応ピット割当ての各技術を用いて高能率符号化する技術について、図5以降を参照しながら説明する。

【0059】図5は本発明に係る実施の形態が適用される音響波形信号の符号化装置の概略構成を示すブロック図である。この実施の形態において、入力された信号波形101は変換手段1101によって信号周波数成分の信号102に変換された後、信号成分符号化手段1102によって各成分が符号化されて信号103となり、符号列生成手段1103によって符号列104が生成される。

【0060】図6は図5の変換手段1101の具体例で、帯域分割フィルタによって二つの帯域に分割された信号がそれぞれの帯域において、MDCT(モディファイド離散コサイン変換)等の順スペクトル変換手段1211、1212によりそれぞれスペクトル信号成分221、222に変換されている。図6の信号201は図5の信号101に対応し、図6の各信号221、222は図5の信号102に対応している。図6の変換手段で、信号211、212の帯域幅は、信号201の帯域幅の1/2となっており、信号201の1/2に間引かれている。もちろん変換手段としてはこの具体例以外にも多数考えられ、例えば、入力信号を直接、MDCTによってスペクトル信号に変換しても良いし、MDCTではなく、DFT(離散フーリエ変換)やDCT(離散コサイン変換)によって変換しても良い。いわゆる帯域分割フィルタによって信号を帯域成分に分割することも可能であるが、本発明の方法は、多数の周波数成分が比較的少ない演算量で得られる上記のスペクトル変換によって周波数成分に変換する方法をとると都合が良い。

【0061】図7は、図5の信号成分符号化手段1102の具体例を示し、各信号成分(信号301)は、正規化手段1301によって所定の帯域毎に正規化が施された後(信号302)、量子化精度決定手段1302によって計算された量子化精度(信号303)に基づいて量子化手段1303によって量子化され、信号304として取り出される。図7の信号301は図5の信号102に対応し、図7の信号304は図5の信号103に対応しているが、ここで、信号304には量子化された信号成分に加え、正規化係数情報や量子化精度情報も含まれている。

【0062】図8は、図5に示す符号化装置によって生成された符号列から音響信号を出力する復号化装置の一例を示すブロック図である。この図8の復号化装置において、符号列401から符号列分解手段1401によって各信号成分の符号402が抽出され、それらの符号402から信号成分復号化手段1402によって各信号成分403が復元された後、逆変換手段1403によって音響波形信号404が出力される。

【0063】図9は、図8の逆変換手段1403の具体例であるが、これは図6の変換手段の具体例に対応したもので、逆スペクトル変換手段1501、1502によって得られた各帯域の信号511、512が帯域合成フィルタ1511によって合成されている。図9の各信号501、502は図8の信号403に対応し、図9の信号521は図8の信号404に対応している。

【0064】図10は図5に示される符号化装置において、従来行なわれてきた符号化の方法について説明を行なうための図である。この図10の例において、スペクトル信号は図6の変換手段によって得られたものであり、図10はMDCTのスペクトルの絶対値をレベルをdBに変換して示したものである。入力信号は所定の時間ブロック毎に64個のスペクトル信号に変換されており、それが図中の[1]から[8]の8つの帯域(以下、これを符号化ユニットと呼ぶ)にまとめて正規化および量子化が行なわれる。量子化精度は周波数成分の分布の仕方によって符号化ユニット毎に変化させることにより、音質の劣化を最小限に押さえる聴覚的に効率の良い符号化が可能である。

【0065】以上述べた方法に対して、さらに符号化効率を高めることが可能である。例えば、量子化されたスペクトル信号のうち、頻度の高いものに対しては比較的短い符号長を割り当て、頻度の低いものに対しては比較的長い符号長を割り当てるこことによって、符号化効率を高めることができる。また例えば、変換ブロック長を長くとることによって、量子化精度情報や正規化係数情報といったサブ情報の量を相対的に削減でき、また周波数分解能を上げるので、周波数軸上で量子化精度をよりこまやかに制御できるため、符号化効率を高めることができる。

【0066】図11は上述のような方法で符号化された信号を記録するための従来技術に基づいたフォーマットの実施の形態を示したものである。この例において、全帯域は全部でB個の帯域に分割されており、低域側から数えてi番め(ただし、 $1 \leq i \leq B$)の帯域の量子化ビット数をW(i)、i番めの帯域の正規化係数をS(i)、i番めの帯域の正規化及び量子化の施されたスペクトル係数のビット列Q(i)の各々が、図11に示す順番で記録されている。

【0067】ここで、本発明の第一の実施の形態は、ソフトの内容を確認できる一部の信号成分には暗号化を施

さす、一般の再生手段でもその内容を試聴できるようにするとともに、さらに高音質の再生を可能にする信号成分に対しては暗号化を施して信号を記録することにより、鍵を入手した者のみが価値の高い高音質の再生が可能になるようするもので、図12は本発明の第一の実施の形態の方法により、符号化を行なう場合の符号列の例を示したものである。

【0068】すなわち、この図12に示す実施の形態においては、入力された情報信号を、内容を把握できる低品質の第一の信号成分としての低域成分と、高品质再生のための第二の信号成分としての高域成分とに分割し、上記第二の信号成分のみを暗号化して符号化している。

【0069】この図12の符号列で図11の符号列と異なるのは、入力情報信号の高域成分に対応するQ(C+1)からQ(B)まで(ただし、 $1 < C < B$)の符号列が、疑似ランダムビット列によって暗号化されて、R(Q(C+1))からR(Q(B))までの符号列として記録されている点である。

【0070】この符号列を図8の復号化装置で再生しようとすると、(C+1)番からB番までの高域の信号は正規化および量子化されたスペクトル係数の別途列が暗号化されているため、正しく再生することができないが、1番からC番までの低域の信号は正しく復号することができる。一般に音響信号の場合、低域の信号に殆どの情報量が集中しているので、このように低域の信号が正しく再生されることにより、試聴者はそのソフトの内容を把握することができるので、これにより、高音質再生のために必要な鍵を購入すべきかどうかの判断を行なうことができる。

【0071】ところで、図12のような符号化方法をとった場合、図8の復号化装置で再生した時に、高域側に不快な雑音がのることになる。そこでそのような欠点を補うような、本発明のより望ましい符号化方法の実施の形態について、図13を参照しながら説明する。

【0072】図13の実施の形態では、図12の実施の形態においてW(C+1)からW(B)の信号が記録されていた部分には、W'(C+1)からW'(B)として0ビット割り当てを行なっていることを示す情報が記録され、W(C+1)からW(B)の信号はこのブロックの信号の最後部に記録されている。また、このW(C+1)からW(B)の信号を記録するために必要な分、正規化および量子化の施されたスペクトル係数のビット列が使用するビット数は図12の例よりも少ないものとして符号化がなされている。

【0073】すなわち、この図13に示す実施の形態においては、入力された情報信号を、内容を把握できる低品質の低域成分と、高品质再生のための高域成分とに分割し、上記高域成分のみを暗号化してR(Q(C+1))からR(Q(B))までの符号列として符号化すると共に、この高域成分に関する情報、例えば量子化ビット数情報を、低品質再生用のW'(C+1)からW'(B)までの第一の符号列と、

高品质再生用のW(C+1)からW(B)までの第二の符号列とに二重に符号化している。

【0074】この図13に示すビット列を図8の復号化装置で再生した場合、この復号化装置は、(C+1)からBまでのバンドにはビットが割り当てられていないものと判断し、R(Q(C+1))からR(Q(B))までの符号列は無いものとして再生を行なうので、図12の例の場合に発生したような不快な雑音は発生せず、ただ、帯域の狭い出力音が再生される。これにより、試聴者は不快な思いを引き起しあしないが、高品质では無い音を試聴してこの鍵を入手すべきかどうかの判断を行なうことができる。

【0075】図14は図13の実施の形態の符号化方法を実現するための符号化手段の具体例を示したもので、この具体例においては、各時間ブロック毎にNビットを使用して符号化された信号が記録媒体に記録されるものとする。

【0076】この図14に示す実施の形態において、入力されたPCM信号601は、変換手段1601によって信号周波数成分の信号602に変換される。次にこの

20 信号602は、図5の符号化装置と同様に、信号成分符号化手段1602によって、所定の帯域毎に正規化及び量子化が施されて符号化される。ここで、図5の符号化装置においては、各量子化ビット数の符号化にM₁ビット、各正規化係数の符号化にM₂ビットが使用されるとして、各時間ブロック毎に正規化および量子化の施されたスペクトル係数のビット列に(N-(M₁+M₂)*B)ビットが使用できるものとしてビット割り当てが行なわれる。これに対して、図14の符号化手段においては、各時間ブロック毎に正規化および量子化の施されたスペクトル係数のビット列に(N-(M₁+M₂)*B-(B-C)*M₃)ビットが使用できるものとしてビット割り当てが行なわれ、その結果が、W(1)からW(B)、S(1)からS(B)、Q(1)からQ(B)として、信号603として出力される。

【0077】また、制御手段1603の生成する鍵信号605を初期値として疑似ランダムビット列発生手段1604が output した疑似ランダムビット列606と信号成分符号化手段1602の出力した信号603との排他的論理和が排他的論理和手段1605によってとられ、その結果が信号607として出力される。符号列生成手段40 1606は、各信号603、607の情報、およびW'(C+1)からW'(B)に相当する0信号を選択的に結合し、図13に示された符号列608を出力する。

【0078】図15は、本発明の実施の形態として、図14の構成の符号化装置によって生成された符号列を高音質再生するための復号化装置の具体例を示したものである。この図15において、符号列分解手段1901は、図13に示されたフォーマットの符号列801から、W(1)からW(B)、S(1)からS(B)、Q(1)からQ(C)およびR(Q(C+1))からR(Q(B))を抜き出し、選択手段1905および、排他的論理和手段1902に送られる。

一方、制御手段1903を介して送られた鍵信号904を初期値として、疑似ランダムビット列発生手段1904は、図14の信号606と同じ疑似ランダムビット列905を発生し、排他的論理手段1902に送る。排他的論理手段1902は各信号902と905との排他的論理和をとり、その結果である信号906を選択手段1905に送る。

【0079】選択手段1905では、信号902のうちR(Q(C+1))からR(Q(B))を信号906に含まれるQ(C+1)からQ(B)に置き換える。その結果である信号907を信号成分符号化手段1906に送る。

【0080】以上は鍵信号が入手されている場合の処理であるが、鍵信号が入手されていない場合には、選択手段1905は、信号902のうち、R(Q(C+1))からR(Q(B))を無視してかわりに0信号を信号成分符号化手段1906に送る。あとは、信号成分符号化手段1906と逆変換手段1907により、図8の復号化手段と同様にPCM信号909が生成され、出力される。

【0081】以上の説明からも明らかなように、上述の方法をとれば、図8の通常の復号手段で再生した場合、または、鍵を入手せずに図15の復号手段で再生した場合には、雑音が発生しないので不快ではないが、再生帯域の狭い、比較的低音質で再生がなされ、鍵を入手して図15の復号手段で再生した場合には、再生帯域の広い高音質再生がなされる。

【0082】なお、図13の符号化方法は、本発明の一実施の形態に過ぎず、例えば、図16のように、Q(C+1)からQ(B)までを暗号化するかわりに、W(C+1)からW(B)を暗号化してR(W(C+1))からR(W(B))を作ることによっても、図13の方法で符号化した場合と同様の効果が得られる。

【0083】図17は、図16の方法で符号化するための処理の流れの例を示すフローチャートであり、ステップS101からステップS103の処理で、S(1)からS(B)、W(1)からW(B)、Q(1)からQ(B)の情報を計算した後、ステップS104においてW(C+1)からW(B)を暗号化してR(W(C+1))からR(W(B))を作り、ステップS105からステップS109の処理でこれらを組み合わせて図16の符号列を生成する。

【0084】一方図18は、図16の符号列から再生すべき帯域の信号成分を生成するための処理の流れの例を示したものである。先ず、ステップS201において低域側のビット数情報W(1)からW(0)を復号化し、次に、ステップS202において全帯域の正規化係数、S(1)からS(B)を復号化し、さらにステップS203において低域側の正規化および量子化されたスペクトル係数、Q(1)からQ(0)を復号化する。次に、ステップS204において鍵が入手済みの場合とそうでない場合に分け、鍵が入手済みであれば、ステップS205に処理が移る。ステップS205では、高域側のビット数情報R(W

(C+1))からR(W(B))を鍵を用いて復号化し、さらにステップS206において、そうして得られたW(C+1)からW(B)を使用してQ(C+1)からQ(B)の情報を復号化し、以上によって得られた情報を使用してステップS207で1番からB番の信号成分を生成する。一方、鍵が入手済みでない場合には、ステップS208において1番からC番の低域側の信号成分のみを生成する。

【0085】以上、本発明の方法に基づいて符号化する別の実施の形態について述べたが、この他にも本発明の実施方法は種々考えられ、例えば、非常に小さい値の正規化係数が符号化可能な場合には、ビット割り当て情報を0にする替わりに、図8の復号化手段が高域側の正規化係数が記録してあると判断する位置に非常に小さい値の正規化係数値を記録し、それとは別に、真の正規化係数を記録しておくようとしても、図8の通常の復号手段で再生した場合、または、鍵を入手せずに再生した場合には、雑音がほとんど無く不快ではないが、再生帯域の狭い比較的低音質の再生がなされ、一方、鍵を入手して再生した場合には、高音質で再生がなされる、という効果が得られる。

【0086】同様に、符号化しているバンド数も記録している場合には、図8の復号化手段がその情報が記録してあると判断する位置に、狭い帯域を表す情報を記録し、真のバンド数情報を他に記録するようにしても良い。これらを含め、符号の一部の情報を多重に記録し、一方の信号を使用した場合のみ、高品質再生が行なえるようにし、そうでない場合には、信号の一部のみの再生が行なえるようにする方法は種々考えられるが、これらはすべて本発明の方法に含まれるものである。

【0087】また、以上、信号を周波数軸方向に分割してその一部を暗号化する方法について述べたが、信号をレベル方向に分割してその一部を暗号化することも可能で、図19、図20はそれぞれ、そのための符号化手段、復号化手段の実施の形態を示したものである。

【0088】すなわち、図19において、入力PCM信号753は信号分割手段1753によって下位側のビット754、および上位側のビット755に分割され、下位側のビット754のみ、排他的論理手段1754によってスクランブルがかけられた後、信号合成手段1755によって再び上位ビットと合成される。一方、図20において、図19の符号化手段の出力757と同じビット列774は、下位側のビット775、および上位側のビット776に分割され、下位側のビット775のみ、排他的論理手段1774によってスクランブルが解除された後、信号合成手段1775によって再び上位ビットと合成され、図19の入力PCM信号753と同じPCM信号778が得られる。

【0089】しかしながら、周波数方向に信号を分割した方がスクランブルが解かれていないと想定して試聴した場合、雑音が聞こえずに違和感は少ない。また、信号圧縮

をかける場合には、下位側のビットの情報は消失することが多いので、周波数方向に対して信号を分割する方が、より広範囲の用途に適用することができる。

【0090】以上、オーディオ信号を用いた場合を例にとって説明を行なったが、本発明の方法は画像信号に対しても適用することが可能である。しかしながら、オーディオ信号の場合、帯域によって適応的にビット割当を行なうことが音質維持のために特に有効であり、そのためのビット割当情報を記録する方法が広く用いられており、本発明の方法を容易かつ有効に適用することが可能である。

【0091】また以上、各曲に対応した鍵情報を暗号化した方法について述べたが、本発明の方法は必ずしも各曲に対応した鍵情報を用いた場合でなくても適用することが可能であり、例えば、非公開の共通アルゴリズムによって高音質再生に必要な情報を符号化することも可能である。この場合、高音質再生のための規格そのものが一種の鍵になっており、本発明の記述における暗号化とはこのような場合を含めたものである。ただし、実際に各曲、あるいは各媒体毎等に鍵情報を使用して管理を行なうことにより、より安全な情報流通処理が可能であることは言うまでもない。

【0092】また以上、符号化されたビットストリームを記録媒体に記録する場合について説明を行なったが、本発明の方法はビットストリームを伝送する場合にも適用可能であり、これにより、例えば、放送されているオーディオ信号を鍵を入手した聴取者のみに高音質再生ができるようにし、その他の聴取者に対してはその内容が十分把握できるが、比較的低音質での再生のみができるようになることが可能である。

【0093】

【発明の効果】以上の説明からも明らかなように、本発明によれば、入力された情報信号を、内容を把握できる程度の低い品質の第一の信号成分と、高品質再生のための第二の信号成分とに分割し、上記第二の信号成分のみを暗号化して符号化することにより、暗号化の鍵情報が無くとも第一の信号成分により内容を把握できる程度の低い品質の再生が行え、鍵情報を用いることにより高品質再生が行える。

【0094】従って、ソフトの内容を確認してから高品質再生に必要な鍵情報を入手すべきかどうかを判断することが可能となり、より円滑なソフトウェアの配布をすることが可能となった。さらに、本発明により、暗号解除の機能を持っていない再生装置を用いても比較的低音質ではあるが、その曲の内容等を知ることができるので、例えば、通勤中に通常の再生装置を用いて試聴を行うことが可能となり、より多くの対象者に対して、それと同じ内容の曲が高音質で記録されているディスクを購入すべきか否か等の判断を下すための試聴を行なわせることが可能になった。さらに本発明の方法により、高

能率符号化を行なう場合にも上述の目的を果たす暗号化が可能になる。

【0095】また、一部の情報、例えば上記第二の信号成分に関する情報については、低品質再生用の第一の符号と高品質再生用の第二の符号とに二重に符号化し、上記第一の符号は暗号化しないことにより、この第一の符号を用いて再生することにより、上記第二の信号成分によるノイズ等の悪影響を受けることなく、低品質の再生が行える。これは、符号化されて得られた符号列が鍵の無い再生手段にとっても意味のある符号列にすることによって、広い範囲の再生装置で比較的低品質の再生を可能にするものである。

【図面の簡単な説明】

【図1】情報信号を暗号化するための構成の一例を示すブロック図である。

【図2】情報信号を暗号化した符号列を復号化するための構成の一例を示すブロック図である。

【図3】暗号化および復号化するための一つの方法を説明するための図である。

20 【図4】本発明の実施の形態が適用される圧縮データ記録及び/又は再生装置の一例の概略構成を示すブロック回路図である。

【図5】本発明の説明に供する符号化装置の一例を示すブロック図である。

【図6】図5の符号化装置の変換手段の具体例を示すブロック図である。

【図7】図5の符号化装置の信号成分符号化手段の具体例を示すブロック図である。

【図8】本発明の説明に供する復号化装置の具体例を示すブロック図である。

30 【図9】図8の復号化装置の逆変換手段の具体例を示すブロック図である。

【図10】本発明の説明に供する符号化方法を説明するための図である。

【図11】本発明の説明に供する符号化方法により得られた符号列の一例を説明するための図である。

【図12】本発明係る符号化方法の実施の形態により得られた符号列の一例を説明するための図である。

【図13】本発明係る符号化方法の他の実施の形態により得られた符号列の一例を説明するための図である。

40 【図14】本発明に係る実施の形態が適用された符号化装置の一例を示すブロック図である。

【図15】本発明に係る復号化装置の実施の形態を示すブロック図である。

【図16】本発明係る符号化方法の他の実施の形態の変形例により得られた符号列の一例を説明するための図である。

【図17】図16の符号列を得るための符号化方法の一例を説明するためのフローチャートである。

50 【図18】図16の符号列を復号化する復号化方法の一

21

例を説明するためのフローチャートである。本発明による復号化方法の実施例を示す流れ図である。

【図19】本発明に係るさらに他の実施の形態が適用された符昌化装置を示すブロック図である。

【図20】本発明に係るさらに他の実施の形態となる復号化装置の一例を示すプロック図である。

考化装置の 【第三回】

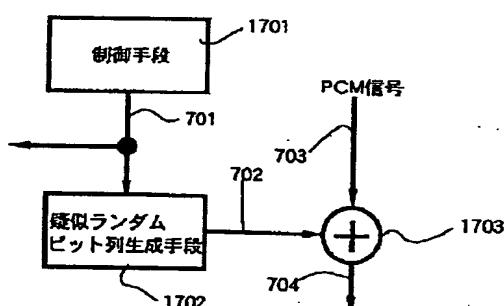
【符号の説明】 1.6.0.1 突撃手段 1.6.0.2 気象成像装置

22

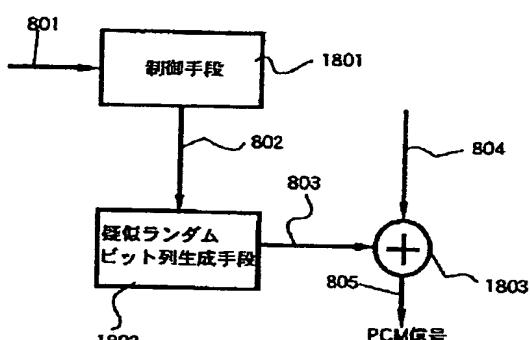
* 段、 1603, 1903, 1751, 1771 制御
 手段、 1604, 1904, 1752, 1772 疑似ランダムビット列発生手段、 1605, 1902,
 1754, 1774 排他的論理和手段、 1601
 符号列生成手段、 1901 符号列分解手段、 19
 05 選択手段、 1906 信号成分復号化手段、
 1907 游奕換手段

22

[圖 1]



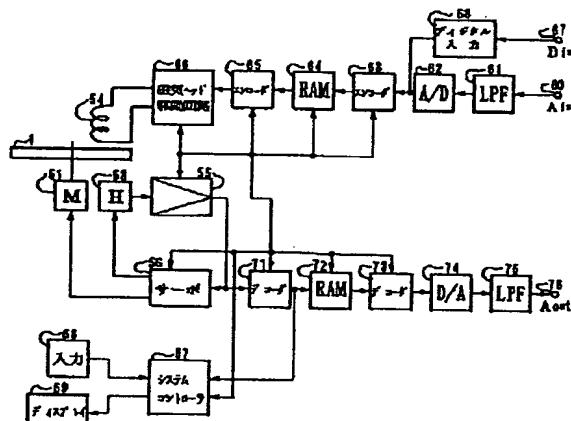
[圖21]



[图3]

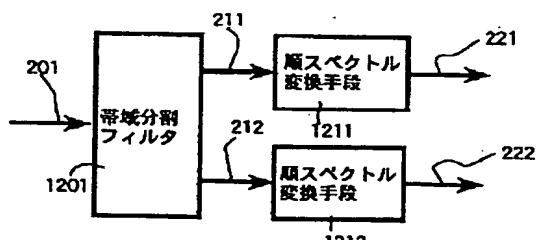
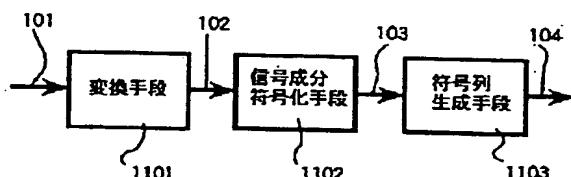
[図4]

A	B	$A \oplus B$	$A \oplus B \oplus B$
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

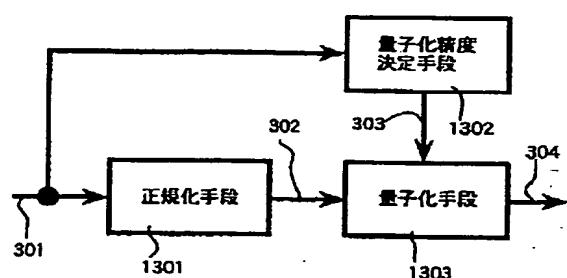


〔圖5〕

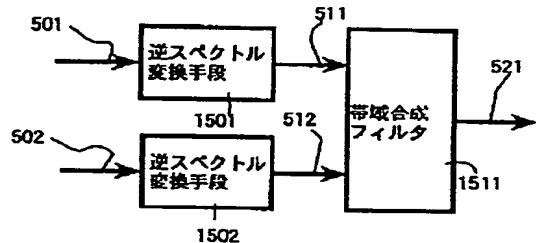
[圖 6]



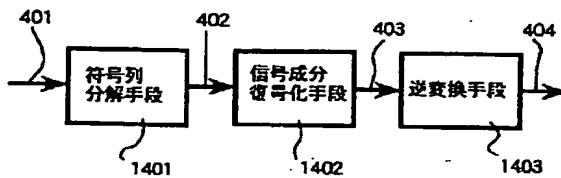
【図7】



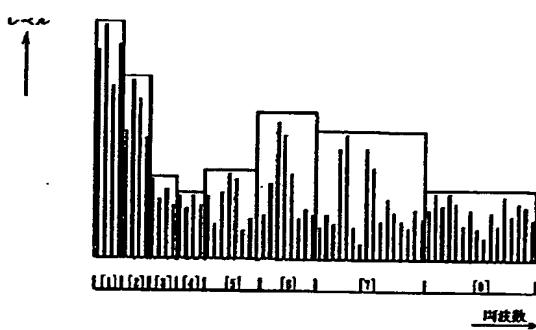
【図9】



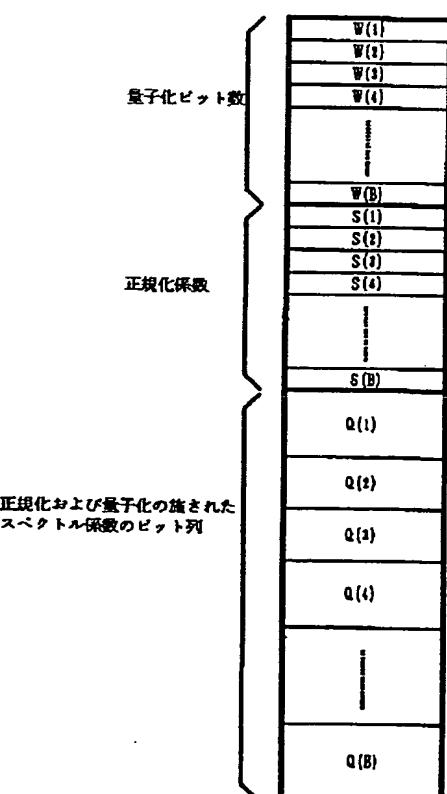
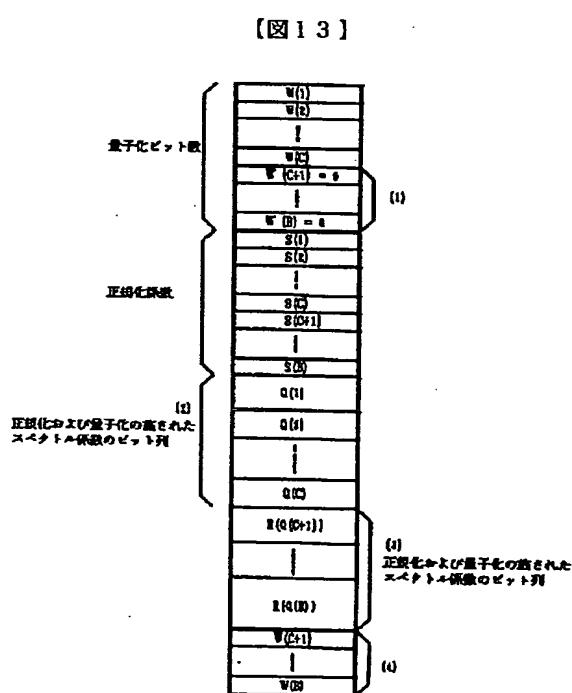
【図8】



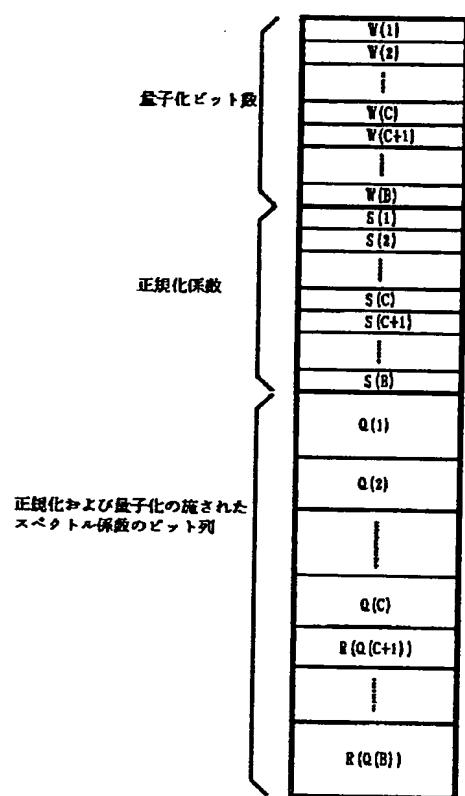
【図10】



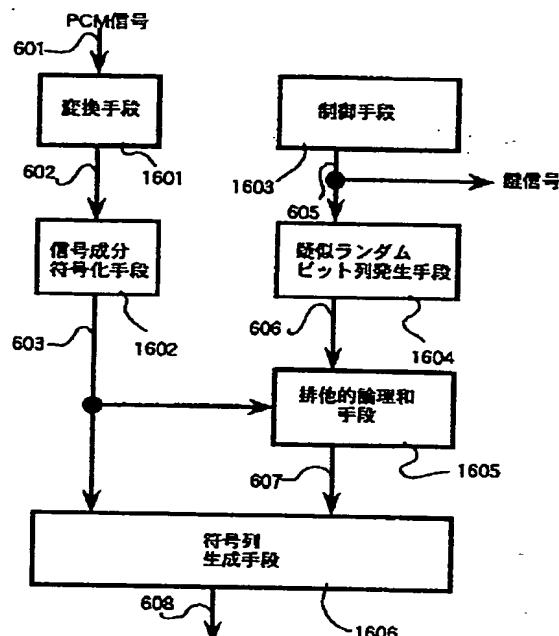
【図11】



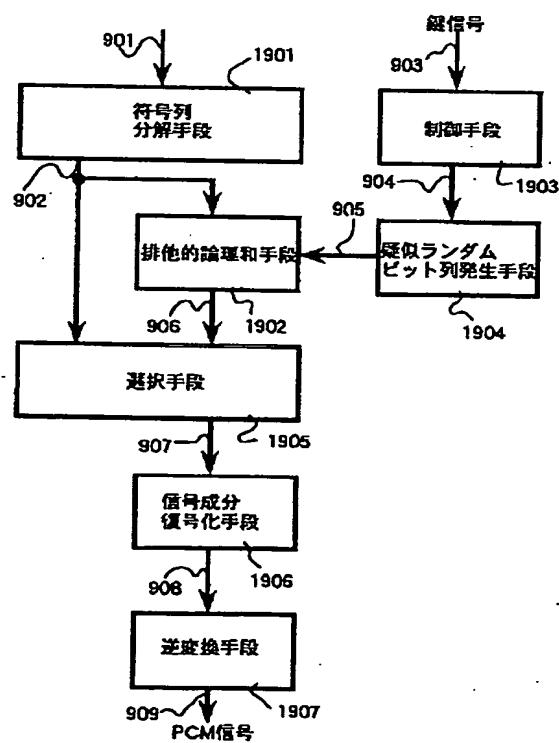
【図12】



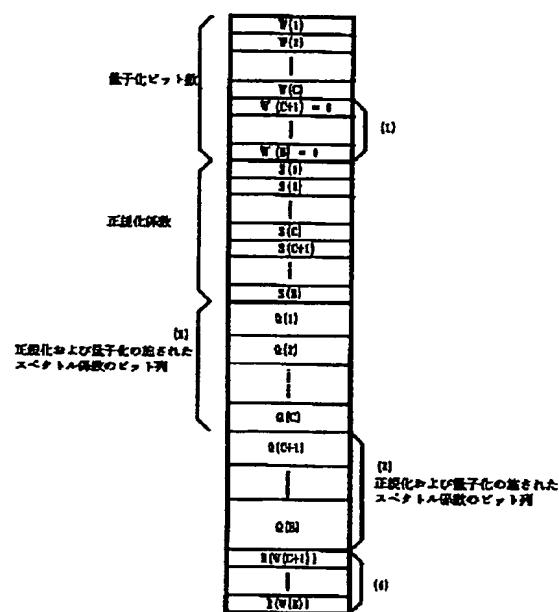
【図14】



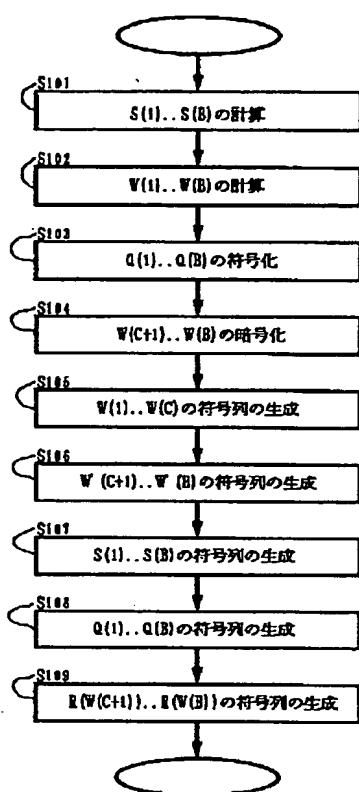
【図15】



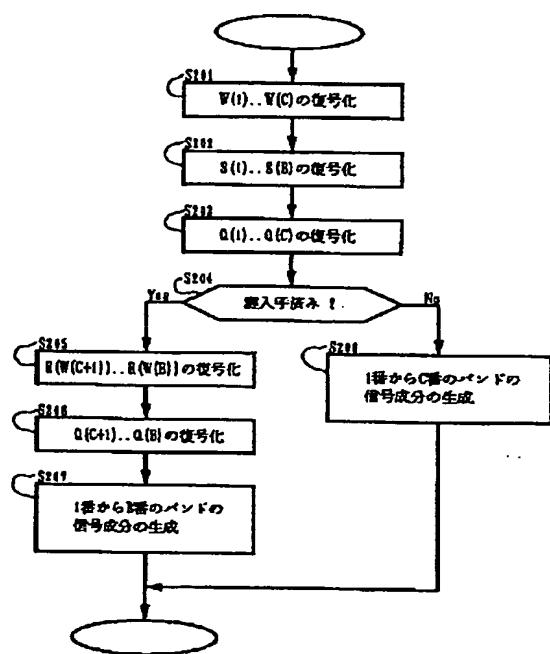
【図16】



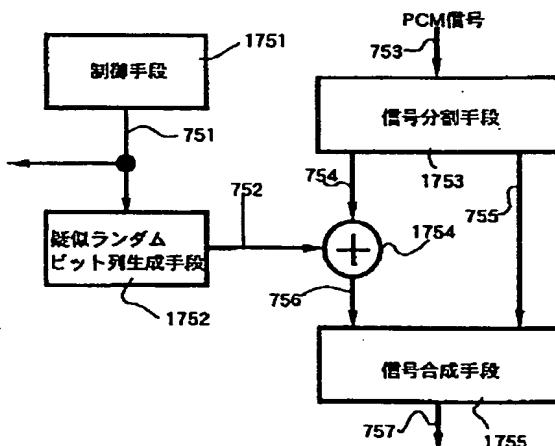
【図17】



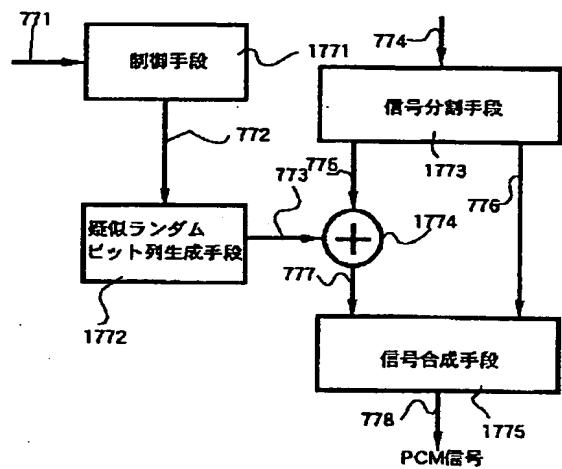
【図18】



【図19】



【図20】



【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第7部門第3区分

【発行日】平成13年4月27日(2001.4.27)

【公開番号】特開平10-135944

【公開日】平成10年5月22日(1998.5.22)

【年通号数】公開特許公報10-1360

【出願番号】特願平8-288542

【国際特許分類第7版】

H04L 9/18

G10L 19/00

G11B 20/10

// H03M 7/30

【F I】

H04L 9/00 651

G10L 9/18 A

G11B 20/10 H

H03M 7/30 Z

【手続補正書】

【提出日】平成12年3月16日(2000.3.16)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 入力された情報信号を、内容を把握できる低品質の第一の信号成分と、高品质再生のための第二の信号成分とに分割する工程と、
上記第二の信号成分のみを暗号化して符号化する工程と
を有すること
を特徴とする情報符号化方法。

【請求項2】 上記第一の信号成分は上記入力情報信号の低域成分であり、上記第二の信号成分は上記入力情報信号の高域成分であること
を特徴とする請求項1記載の情報符号化方法。

【請求項3】 上記符号化は入力信号を圧縮するように
符号化するものであること
を特徴とする請求項1記載の情報符号化方法。

【請求項4】 一部の情報は低品質再生用の第一の符号と高品质再生用の第二の符号とに二重に符号化され、上記第一の符号は暗号化しないこと
を特徴とする請求項1記載の情報符号化方法。

【請求項5】 情報信号が、内容を把握できる低品質の第一の信号成分と、高品质再生のための第二の信号成分とに分割され、上記第二の信号成分のみが暗号化されて
符号化されていること
を特徴とする記録媒体。

【請求項6】 上記第一の信号成分は上記入力情報信号の低域成分であり、上記第二の信号成分は上記入力情報信号の高域成分であること
を特徴とする請求項5記載の記録媒体。

【請求項7】 上記符号化は入力信号を圧縮するように
符号化するものであること
を特徴とする請求項5記載の記録媒体。

【請求項8】 一部の情報は低品質再生用の第一の符号と高品质再生用の第二の符号とに二重に符号化され、上記第一の符号は暗号化しないこと
を特徴とする請求項5記載の記録媒体。

【請求項9】 情報信号が、内容を把握できる低品質の第一の信号成分と、高品质再生のための第二の信号成分とに分割され、上記第二の信号成分のみが暗号化されて
符号化された符号化信号が供給され、
上記暗号化の鍵信号の有無によって上記符号化信号の内の上記第二の信号成分を復号化するか否かを選択すること
を特徴とする復号化装置。

【請求項10】 上記第一の信号成分は上記入力情報信号の低域成分であり、上記第二の信号成分は上記入力情報信号の高域成分であること
を特徴とする請求項9記載の復号化装置。

【請求項11】 上記符号化は、一部の情報は低品質再生用の第一の符号と高品质再生用の第二の符号とに二重に符号化され、上記第一の符号は暗号化しないこと
を特徴とする請求項9記載の復号化装置。

【請求項12】 上記符号化は入力信号を圧縮するよう
に符号化するものであること
を特徴とする請求項9記載の復号化装置。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0019

【補正方法】変更

【補正内容】

【0019】また、いわゆるMPEG規格の ISO/IEC 1

1172-3:1993(E)、1993においては、帯域によって量子化精度情報を表すビット数が異なるように設定された高能率符号化方式が記述されており、高域になるにしたがって、量子化精度情報を表すビット数が小さくなるように規格化されている。

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-135944

(43)Date of publication of application : 22.05.1998

(51)Int.CI.

H04L 9/18
G10L 9/18
G11B 20/10
// H03M 7/30

(21)Application number : 08-288542

(71)Applicant : SONY CORP

(22)Date of filing : 30.10.1996

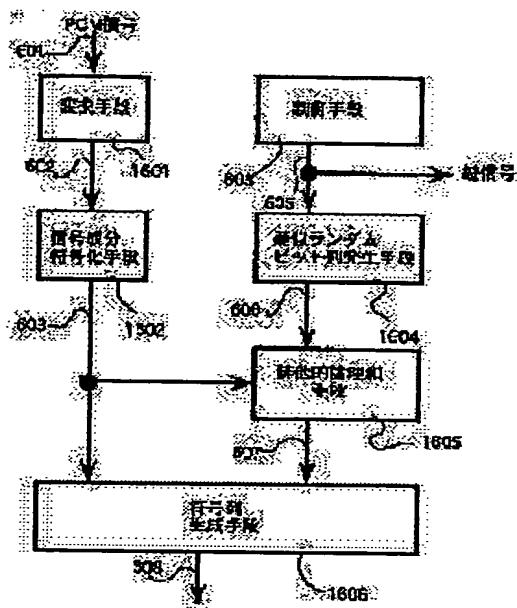
(72)Inventor : TSUTSUI KIYOUYA

(54) INFORMATION CODING METHOD, RECORDING MEDIUM AND DECODER

(57)Abstract:

PROBLEM TO BE SOLVED: To reproduce an information signal at low quality, even when key information for encryption is not available.

SOLUTION: A received PCM signal is converted into a frequency signal component by a conversion means 1601, coded by a signal component coding means 1602, a high-frequency component is fed to an exclusive OR means 1605, in which the high-frequency component is exclusively ORed with a pseudo-random bit stream from a pseudo-random bit stream generating means 1604. A code string generating means 1606 generates a code string 608 having a low-frequency component from the signal component coding means with an encrypted high-frequency component from the exclusive OR means 1605.



LEGAL STATUS

[Date of request for examination] 16.03.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3496411

[Date of registration] 28.11.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C) 1998,2003 Japan Patent Office

*** NOTICES ***

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] The information coding approach characterized by having the process which divides the inputted information signal into the first signal component of low quality which can grasp the contents, and the second signal component for high quality playback, and the process which enciphers only the second signal component of the above and is encoded.

[Claim 2] It is the information coding approach according to claim 1 which the first signal component of the above is a low-pass component of the above-mentioned input signal, and is characterized by the second signal component of the above being a high-frequency component of the above-mentioned input signal.

[Claim 3] The above-mentioned coding is the information coding approach according to claim 1 characterized by being what encoded so that an input signal may be compressed.

[Claim 4] It is the information coding approach according to claim 1 which a part of information is encoded by the duplex at the first sign for low quality playback, and the second sign for high quality playback, and is characterized by not enciphering the first sign of the above.

[Claim 5] The above-mentioned signal is the information coding approach according to claim 1 characterized by being an acoustic signal.

[Claim 6] The record medium characterized by dividing an information signal into the first signal component of low quality which can grasp the contents, and the second signal component for high quality playback, and enciphering and encoding only the second signal component of the above.

[Claim 7] It is the record medium according to claim 6 which the first signal component of the above is a low-pass component of the above-mentioned input signal, and is characterized by the second signal component of the above being a high-frequency component of the above-mentioned input signal.

[Claim 8] The above-mentioned coding is a record medium according to claim 6 characterized by being what encoded so that an input signal may be compressed.

[Claim 9] It is the record medium according to claim 6 which a part of information is encoded by the duplex at the first sign for low quality playback, and the second sign for high quality playback, and is characterized by not enciphering the first sign of the above.

[Claim 10] The above-mentioned signal is a record medium according to claim 6 characterized by being an acoustic signal.

[Claim 11] Decryption equipment characterized by choosing whether an information signal is divided into the first signal component of low quality which can grasp the contents, and the second signal component for high quality playback, the coded signal by which only the second signal component of the above was enciphered and encoded is supplied, and the second signal component of the above of the above-mentioned coded signals is decrypted by the existence of the key signal of the above-mentioned encryption.

[Claim 12] It is decryption equipment according to claim 11 which the first signal component of the above is a low-pass component of the above-mentioned input signal, and is characterized by the second signal component of the above being a high-frequency component of the above-mentioned input signal.

[Claim 13] It is decryption equipment according to claim 11 which the first signal component of the above is a low-pass component of the above-mentioned input signal, and is characterized

by the second signal component of the above being a high-frequency component of the above-mentioned input signal.

[Claim 14] The above-mentioned coding is decryption equipment according to claim 11 characterized by being what encoded so that an input signal may be compressed.

[Claim 15] The above-mentioned signal is decryption equipment according to claim 11 characterized by being an acoustic signal.

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the information coding approach which enciphers information signals, such as an audio PCM signal, and is encoded, the record medium with which the encoded signal was recorded, and the decryption equipment which decrypts a coded signal.

[0002]

[Description of the Prior Art] For example, information signals, such as an acoustic signal and a video signal, are enciphered and broadcast, or it records on a record medium, and the circulation approach of the software of permitting the viewing and listening only to those who purchased the key is learned. As the approach of encryption, the initial value of a random-number sequence is given as a key signal to the bit string of the acoustic signal of PCM, and the approach of transmitting the bit string which took the exclusive OR of the random-number sequence of 0/1 and the bit string of Above PCM which were generated, or recording on a record medium is learned, for example. Only those who received the key signal enable it to reproduce that acoustic signal correctly, and only a noise can be prevented from reproducing those who did not receive a key signal by using this approach.

[0003] On the other hand, an acoustic signal is compressed and broadcast, or the approach of recording on a record medium has spread, and record media, such as a magneto-optic disk which can record signals, such as an encoded audio or voice, are used widely. Although it is in the technique of high efficiency coding of signals, such as an audio or voice, variously For example, it is the deblocking frequency band division method divided and encoded to two or more frequency bands without blocking the audio signal on a time-axis etc. Band division coding (sub band coding: SBC), the blocking frequency band division method which changes the signal of a time-axis into the signal on a frequency shaft (spectrum conversion), divides into two or more frequency bands, and is encoded for every band, the so-called conversion coding, etc. can be mentioned. Moreover, the technique of high efficiency coding which combined above-mentioned band division coding and above-mentioned conversion coding is also considered, in this case, after performing band division by the above-mentioned band division coding, spectrum conversion of the signal for this every band is carried out at the signal on a frequency shaft, and coding is performed for each [by which spectrum conversion was carried out] of this band of every.

[0004] Here, as a filter mentioned above, there is a QMF filter, for example and it is reference "1976, R.E.Crochiere, Digital coding of speech in subbands, Bell Syst.Tech.J.Vol.55, and No.8 1976" about this QMF filter. It is stated, moreover, reference "ICASSP 83, BOSTON Polyphase Quadrature filters—A new subband coding technique, and Joseph H.Rothweiler" **** — the filter division technique of a ** bandwidth is described.

[0005] Here, as spectrum conversion mentioned above, an input audio signal is blocked by predetermined unit time amount (frame), for example, and there is spectrum conversion which changes a time-axis into a frequency shaft by performing discrete Fourier transform (DFT), cosine conversion (DCT), MODIFAIIDO DCT conversion (MDCT), etc. for every block concerned. About MDCT, it is reference "ICASSP 1987, Subband/Transform Coding Using Filter Bank Designs Based on Time Domain Aliasing Cancellation, and J.P.Princen A.B.Bradley, Univ.of

Surrey, and Royal Melbourne Inst.of Tech.". It is stated.

[0006] When above-mentioned DFT and above-mentioned DCT are used as an approach of changing a wave signal into a spectrum, if it changes with the time amount block which consists of M samples, M independent real data will be obtained. In order to mitigate the connection distortion during a time amount block, it is [neighboring blocks and] usually M1, respectively. Since an individual makes it overlap a sample every, at DFT or DCT, it is on the average. (M-M1) To the sample of an individual, M real data will be quantized and it will encode.

[0007] On the other hand, when above-mentioned MDCT is used as an approach of changing into a spectrum, since M independent real data is obtained from the 2M piece sample made to overlap neighboring time amount N pieces at a time, it averages, and in MDCT, to M samples, M real data will be quantized and it will encode. In decryption equipment, a wave signal can be reconfigured by adding making the wave element obtained from the sign which did in this way and was obtained using MDCT by performing inverse transformation in each block interfere mutually.

[0008] By generally lengthening the time amount block for conversion, the frequency resolution of a spectrum increases and energy concentrates on a specific spectrum component. Therefore, when neighboring blocks are made to overlap by one half, it changes by the long block length and the number of the spectrum signal moreover acquired uses MDCT which does not increase to the number of the original time amount sample, it becomes possible to perform efficient coding from the case where DFT and DCT are used. Moreover, the interblock distortion of a wave signal is also mitigable by giving sufficiently long overlap to adjoining blocks.

[0009] thus, the band which a quantizing noise generates by quantizing the signal divided for every band by the filter or spectrum conversion — being controllable — properties, such as a masking effect, — using — an acoustic sense —like — more — high — efficiency coding can be performed. before [moreover,] quantizing here — every band — for example, — if it is made to normalize at the maximum of the absolute value of the signal component in the band — further — high — efficiency coding can be performed.

[0010] As frequency-division width of face which quantizes each frequency component by which frequency band division was carried out, band division which took into consideration human being's acoustic-sense property, for example is performed. That is, in the higher region currently generally called the critical band (critical band), bandwidth may divide an audio signal into the band of plurality (for example, 25 bunt) with bandwidth which becomes large. Moreover, in case the data for every band at this time are encoded, predetermined bit allocation or coding according to accommodative bit allocation (bit allocation) the whole band is performed for every band. For example, in case the multiplier data which MDCT processing was carried out [above-mentioned] and obtained are encoded by the above-mentioned bit allocation, coding will be performed with the accommodative allocation number of bits to the MDCT multiplier data for every band obtained by MDCT processing for every above-mentioned block.

[0011] As the technique of such bit allocation, it is reference "Adaptive Transform Coding of Speech Signals and R.Zelinski and P.Noll". And two technique indicated by reference "IEEE Transactions of Acoustics, Speech, and Signal Processing, vol.ASSP-25, No.4, and August 1977" is known.

[0012] In the technique indicated by these reference, bit allocation is performed based on the magnitude of the signal for every band. Although a quantizing-noise spectrum becomes flat and serves as noise energy min by this method, since the masking effect is not used in auditory sensation, an actual feeling of a noise is not the optimal.

[0013] Moreover, the technique of obtaining the required S/N for every band and performing fixed bit allocation by using auditory masking, is described by reference "ICASSP 1980, The critical band coder—digital encoding of the perceptual requirements of the auditory system, M.A.Krassner, and MIT." However, by this technique, even when measuring a property in a sine wave input, since bit allocation is fixed, a characteristic value does not turn into so good a value.

[0014] A part for the fixed bit allocation pattern at which all the bits that can be used for bit allocation were beforehand appointed for every smallness block in order to solve these

problems, Division use is carried out at the part which performs bit allocation depending on the magnitude of the signal of each block, and it is made to depend for the split ratio on the signal related to an input signal, and the high-efficiency-coding equipment which enlarges the rate of split ratio for said fixed bit allocation pattern is proposed, so that the spectrum of said signal is smooth.

[0015] According to this approach, like a sine wave input, when energy concentrates on a specific spectrum, the whole signal-to-noise property can be remarkably improved by assigning many bits to the block containing that spectrum. It is effective in it not only only raising the numeric value on measurement, but improving tone quality on audibility by generally, using such an approach to a signal with a steep spectrum component, since human being's acoustic sense is very sensitive to improve a signal-to-noise property.

[0016] if many ways are proposed by the approach of bit assignment in addition to this, the model about an acoustic sense is elaborated further and the capacity of coding equipment goes up — an acoustic sense —like — seeing — more — high — efficiency coding is attained. In these approaches, it is common to calculate the bit quota reference value of the real number which realizes as faithfully as possible the signal-to-noise property searched for by count, to assign the integral value which approximates it, and to consider as the number of bits.

[0017] Moreover, it sets on the specification and drawing of application of Japanese Patent Application No. No. 500482 [seven to] which this artificer etc. proposed previously. From the spectrum signal, on audibility, especially, the component of important tone nature, i.e., the signal component which energy is concentrating on the outskirts of a frequency of specification, is separated, and the approach of encoding apart from other spectrum components is indicated. By this It is possible to encode an audio signal etc. efficiently with high compressibility, without producing most degradation on audibility.

[0018] What is necessary is in constituting an actual sign train, to encode quantization precision information and normalization multiplier information with the predetermined number of bits for every band where normalization and quantization are performed, next just to encode first, the spectrum signal normalized and quantized.

[0019] Moreover, the so-called MPEG specification In ISO/IEC 11172-3:1993 (E) and a993, it is standardized so that the number of bits showing quantization precision information may become small, as the low bit rate coding method set up so that the numbers of bits which express quantization precision information by the band might differ is described and it becomes a high region.

[0020] Since the relation between normalization multiplier information and quantization precision information is decided when specification is set up, it becomes impossible furthermore, to introduce control of the quantization precision based on a prospective still more advanced acoustic-sense model by this approach, although the method of determining quantization precision information from normalization multiplier information is also learned in decryption equipment instead of encoding quantization precision information directly. Moreover, when width of face is in the compressibility to realize, the need of defining the relation between normalization multiplier information and quantization precision information for every compressibility comes out.

[0021] Next, it is reference "D.A.Huffman about the quantized spectrum signal. : A Method for Construction of Minimum Redundancy Codes, Proc.I.R.E., 40, and p.1098 How to encode more efficiently is also learned by encoding using the variable-length sign described." (1952)

[0022] It is also possible to encipher it as the case of a PCM signal similarly, and to distribute the signal encoded as mentioned above, and those who have not received the key signal in this case cannot reproduce the original signal. Moreover, after changing a PCM signal into a random signal rather than enciphering the encoded bit string, there is also a method of performing coding for compression, and those who have not received the key signal in this case, either can reproduce only a noise.

[0023]

[Problem(s) to be Solved by the Invention] However, by these scramble approaches, when there is no key, or when it is made to reproduce with the usual playback means, if it is reproduced, it cannot become a noise and contents grasp of the software cannot be carried out for this

reason — for example, it was not able to use for the application of distributing the disk which recorded music qualitatively of bass comparatively, purchasing a key only to that by which those who tried listening it went into their mind, and enabling it to newly purchase the disk recorded qualitatively of loud sound after enabling it to reproduce or trying listening that software qualitatively of loud sound.

[0024] Moreover, when enciphering conventionally the signal which gave high efficiency coding, it was difficult [it] to make it not lower the compression efficiency, giving the sign train which is meaningful for the usual playback means. That is, when a scramble is applied to the sign train which gave high efficiency coding and was able to do it as mentioned above, even if it reproduces the sign train, when the sign train a noise not only occurs, but made by scramble does not conform to the specification of the original high efficiency sign, a playback means cannot operate at all.

[0025] Moreover, since there is not necessarily nothing conversely at the reason the signal which applied the scramble to the PCM signal is reproducible when high efficiency coding is carried out, amount of information is deleted using the property of an acoustic sense, and the high efficiency coding is canceled after applying a scramble to a PCM signal, it will become difficult to cancel a scramble correctly. For this reason, even if effectiveness fell as the compressive approach, the approach which a scramble can lift correctly needed to be chosen.

[0026] when this invention is made in view of such the actual condition, and encipher and transmit, or record information signals, such as an audio signal and a video signal, on a record medium and supplying them, it does not have the key of encryption — ** — it aims at offering the information coding approach that playback of low quality which is extent which can check the contents can be performed, and high playback of quality can perform more by using a key, a record medium, and decryption equipment.

[0027]

[Means for Solving the Problem] In order to solve the technical problem mentioned above, the information coding approach concerning this invention divides the inputted information signal into the first signal component of quality with low extent which can grasp the contents, and the second signal component for high quality playback, and is characterized by enciphering only the second signal component of the above and encoding.

[0028] The contents are divided into the first signal component which can be grasped enough, and the second signal component for high quality playback although it is comparatively low quality about a signal. Namely, the first signal component of them While enabling it to reproduce a scramble etc. also with a playback means without the discharge function of encryption, with the playback means which received the key for decoding it, high quality playback is enabled by enabling it to reproduce also including the second signal component.

[0029] This invention is applicable to the record medium which records the signal with which such coding was performed and changes.

[0030] An information signal is divided into the first signal component of low quality which can grasp the contents, and the second signal component for high quality playback, the coded signal by which only the second signal component of the above was enciphered and encoded is supplied, and the decryption equipment concerning this invention is characterized by choosing whether the second signal component of the above of the above-mentioned coded signals is decrypted by the existence of the key signal of the above-mentioned encryption.

[0031] Here, it is mentioned that it is what is encoded so that the above-mentioned coding may compress an input signal. Moreover, a part of information is encoded by the duplex at the first sign for low quality playback, and the second sign for high quality playback, and not enciphering the first sign of the above is mentioned. As a part of these information, the information about the second signal component of the above is mentioned. Furthermore, it is mentioned that the above-mentioned signal is an acoustic signal.

[0032] Moreover, this invention applies encryption, after carrying out high efficiency coding of the signal, but when the sign train which made it such and was made makes it the sign train which is meaningful also for a playback means without a key, it enables playback of comparatively the low quality in the regenerative apparatus of the large range.

[0033]

[Embodiment of the Invention] Hereafter, the gestalt of desirable operation of the information coding approach concerning this invention, a record medium, and decryption equipment is explained, referring to a drawing.

[0034] First, the technique of encryption used for this invention is explained, referring to drawing 1 thru/or drawing 3.

[0035] Drawing 1 is the block diagram showing the example of a configuration of the encryption equipment for generating the enciphered bit string. With this encryption equipment, a bit string 704 is outputted by taking an exclusive OR with the output 702 of the pseudo-random bit string generating means 1702 generated using the initial value information 701 for which each bit of the PCM signal 703 which is an input signal was sent to the exclusive-OR means 1703 from delivery and a control means 1701. As the bit of No. 50 is chosen, it can consist of under the random number sequence from which die length repeats actuation of squaring it by making into initial value the bit string chosen as the arbitration which is 100 bits, and leaving only 100 bits of a center, and is obtained as a pseudo-random bit string generating means 1702, for example. thus, it sees, although the right key (in this case, initial value information 701) came to hand, and it can make it possible to reproduce the original PCM signal by recording the outputted bit string on an optical disk.

[0036] Drawing 2 shows the example of a configuration of the decryption equipment for decrypting the bit string 704 which the encryption equipment of drawing 1 outputted. If the pseudo-random bit string generating means 1802 has the same function as the pseudo-random bit string generating means 1702 of drawing 1, therefore the same key signal is given as initial value, the same pseudo-random bit string will be obtained. As for this pseudo-random bit string 803 and input signal 804, an exclusive OR is taken. Since Bit A will be reproduced if an exclusive OR with Bit B is twice taken to Bit A as shown in drawing 3 here, when the right key signal comes to hand, a bit string 805 can be reproduced correctly. In the example of drawing 2, the key information 801 is supplied to a control means 1801, and a control means 1801 is sending the initial value information 802 equal to the initial value information 701 from the control means 1701 of above-mentioned drawing 1 to the pseudo-random bit string generating means 1802, it makes the pseudo-random bit string generating means 1802 generate the same pseudo-random bit string as the time of encryption of drawing 1, and is sent to the exclusive-OR means 1803.

[0037] However, since the contents of the software currently recorded on media, such as a disk, could not be known at all unless the right key signal came to hand when encryption which was mentioned above on the whole to the PCM signal which is an input signal was given, it was difficult to judge whether a key signal for those who received the disk to decode it should be purchased. For this reason, software was not able to be distributed, for example at a cheap price, and the user who tried listening it was not able to say that he purchased a key signal only to the thing included in mind.

[0038] Then, in order to solve such a problem, in the gestalt of operation of this invention, the PCM signal which is an input signal was divided into two signal components, and only one side was enciphered and it has encoded. About these two signal components, the low-pass component of the inputted PCM signal is made into the first signal component, and enciphering only the second signal component is mentioned considering a high-frequency component as the second signal component.

[0039] Here, an example of the compressed data record and/or the regenerative apparatus with which the gestalt of desirable operation of this invention is applied is explained, referring to drawing 4.

[0040] In the compressed data record and/or the regenerative apparatus which are shown in drawing 4, the magneto-optic disk 1 by which a rotation drive is carried out with a spindle motor 51 is used as a record medium. At the time of record of the data to a magneto-optic disk 1, by impressing the modulation field according to record data by the magnetic head 54, where a laser beam is irradiated by the optical head 53, the so-called field modulation record is performed and data are recorded along the recording track of a magneto-optic disk 1. Moreover, at the time of playback, the recording track of a magneto-optic disk 1 is traced by the laser beam by the optical head 53, and it reproduces in magneto-optics.

[0041] The optical head 53 consists of photodetectors which have the light sensing portion of optics, such as laser light sources, such as a laser diode, a collimator lens, an objective lens, a polarization beam splitter, and a cylindrical lens, and a predetermined pattern. This optical head 53 is formed in the above-mentioned magnetic head 54 and the location which counters through the magneto-optic disk 1. When recording data on a magneto-optic disk 1, while driving the magnetic head 54 by the head drive circuit 66 of the recording system mentioned later and impressing the modulation field according to record data, a field modulation technique performs heat magnetic recording by irradiating a laser beam on the purpose track of a magneto-optic disk 1 by the optical head 53. Moreover, this optical head 53 detects the reflected light of the laser beam which irradiated the purpose track, detects a focal error by the so-called astigmatism method, for example, detects a tracking error by the so-called push pull method. When reproducing data from a magneto-optic disk 1, the optical head 53 detects the difference in the polarization angle (car angle of rotation) of the reflected light from the purpose track of a laser beam, and generates a regenerative signal at the same time it detects the above-mentioned focal error and a tracking error.

[0042] The output of the optical head 53 is supplied to the RF circuit 55. This RF circuit 55 is supplied to the decoder 71 of the reversion system which makes a regenerative signal binary and mentions it later while it extracts the above-mentioned focal error signal and a tracking error signal from the output of the optical head 53 and supplies them to the servo control circuit 56.

[0043] The servo control circuit 56 consists of for example, a focus servo control circuit, a tracking servo control circuit, a spindle motor servo control circuit, a thread servo control circuit, etc. The above-mentioned focus servo control circuit performs focal control of the optical system of the optical head 53 so that the above-mentioned focal error signal may become zero. Moreover, the above-mentioned tracking servo control circuit performs tracking control of the optical system of the optical head 53 so that the above-mentioned tracking error signal may become zero. Furthermore, the above-mentioned spindle motor servo control circuit controls a spindle motor 51 to carry out the rotation drive of the magneto-optic disk 1 with a predetermined rotational speed (for example, constant linear velocity). Moreover, the above-mentioned thread servo control circuit moves the optical head 53 and the magnetic head 54 to the purpose track location of a magneto-optic disk 1 specified by the system controller 57. The servo control circuit 56 which performs such various control action sends the information which shows the operating state of each part controlled by this servo control circuit 56 to a system controller 57.

[0044] The key input control unit 58 and the display 59 are connected to the system controller 57. This system controller 57 performs control of a recording system and a reversion system by actuation input with the actuation input by the key input control unit 58. Moreover, a system controller 57 manages the record location and playback location on the above-mentioned recording track which the optical head 53 and the magnetic head 54 are tracing based on the address information of the sector unit reproduced with a header time, Q data of a sub-code, etc. from the recording track of a magneto-optic disk 1. Furthermore, a system controller 57 performs control to which playback time amount is displayed on a display 59 based on the data compression rate of this compressed data record regenerative apparatus, and the playback positional information on the above-mentioned recording track.

[0045] By carrying out the multiplication of the inverse number (for example, the time of 1/4 compression 4) of a data compression rate to the address information (absolute time information) of the sector unit reproduced from the recording track of a magneto-optic disk 1 with the so-called header time, the so-called sub-code Q data, etc., this playback time amount display searches for an actual hour entry, and displays this on a display 59. In addition, when absolute time information is beforehand recorded, for example on recording tracks, such as a magneto-optic disk, at the time of record (preformatted), it is also possible to display the current position by actual chart lasting time by reading this preformatted absolute time information and carrying out the multiplication of the inverse number of a data compression rate.

[0046] Next, in the recording system of the disk record / regenerative apparatus shown in this

drawing 4, the analog audio input signal Ain from an input terminal 60 is supplied to A/D converter 62 through a low pass filter 61, and this A/D converter 62 quantizes the above-mentioned analog audio input signal Ain. The digital audio signal obtained from A/D converter 62 is ATC (adaptive transform coding: Adaptive Transform Coding). An encoder 63 is supplied. Moreover, the digital audio input signal Din from an input terminal 67 is supplied to the ATC encoder 63 through the digital input interface circuitry 68. The compressed data (ATC data) which the ATC encoder 63 performs bit compression (data compression) processing according to a predetermined data compression rate about the digital audio PCM data of the predetermined transfer rate which quantized the above-mentioned input signal Ain with above-mentioned A/D converter 62, and is outputted from the ATC encoder 63 is supplied to memory 64. For example, if the case where a data compression rate is 1/8 is explained, the data transfer rate here is reduced by one eighth of the so-called data transfer rates (75 sectors / second) of the CD-DA format which is a format of the standard digital audio CD (9.375 sectors / second).

[0047] Next, writing and read-out of data are controlled by the system controller 57, and memorize temporarily the ATC data supplied from the ATC encoder 63, and memory (RAM) 64 is used as buffer memory for recording on a disk if needed. That is, for the compression audio data supplied from the ATC encoder 63 when a data compression rate is 1/8, for example, that data transfer rate is 1/8 of the standard data transfer rate (75 sectors / second) of a CD-DA format, 9.375 [i.e.,]. It decreases at the sector/second and this compressed data is continuously written in memory 64. If 1 sector per 8 sectors is recorded as having mentioned above this compressed data (ATC data), it is sufficient, but since it is next to impossible as a matter of fact, such record of every 8 sectors is made to record sector continuation which is mentioned later.

[0048] This record is burstily performed through an idle period with the same data transfer rate (75 sectors / second) as a standard CD-DA format by making into a record unit the cluster which consists of predetermined two or more sectors (for example, 32 sector + number sector). That is, in memory 64, the ATC audio data of the data compression rates 1/8 continuously written in with the low transfer rate of the 9.375 (= 75/8) sectors / second according to the above-mentioned bit compression rate are burstily read with the transfer rate of the above-mentioned 75 sectors / second as record data. the instant-data transfer rate within the time amount of the record actuation burstily performed although the overall data transfer rate containing a record idle period is the low rate of the above-mentioned 9.375 sectors / second about this data read and recorded — the above — standard 75 sectors / second have come. Therefore, when it is the same rate (constant linear velocity) as the CD-DA format with a standard disk rotational speed, record of the same recording density as this CD-DA format and a storage pattern will be performed.

[0049] it is supplied to an encoder 65, the ATC audio data, i.e., the record data, burstily read from memory 64 with the transfer rate (an instant —like) of the above-mentioned 75 sectors / second. Here, the unit by which continuation record is carried out by one record in the data stream supplied to an encoder 65 from memory 64 is made into the number sector for cluster connection allotted to this cluster [which consists of two or more sectors (for example, 32 sectors)], and cluster order location. This sector for cluster connection is set up for a long time than the interleave length in an encoder 65, and even if it interleaves, he is trying not to affect the data of other clusters.

[0050] An encoder 65 performs coding processing (parity addition and interleave processing), EFM coding processing, etc. for an error correction about the record data burstily supplied as mentioned above from memory 64. The record data with which coding processing by this encoder 65 was performed are supplied to the magnetic-head drive circuit 66. The magnetic head 54 is connected, and this magnetic-head drive circuit 66 drives the magnetic head 54 so that the modulation field according to the above-mentioned record data may be impressed to a magneto-optic disk 1.

[0051] Moreover, a system controller 57 controls a record location to record continuously the above-mentioned record data burstily read from memory 64 by this memory control on the recording track of a magneto-optic disk 1 while performing memory control like **** to memory

64. Control of this record location manages the record location of the above-mentioned record data burstily read from memory 64 by the system controller 57, and is performed by supplying the control signal which specifies the record location on the recording track of a magneto-optic disk 1 to the servo control circuit 56.

[0052] Next, the reversion system of the disk record / regenerative apparatus shown in drawing 4 is explained. the playback output which this reversion system is for reproducing the record data continuously recorded by the above-mentioned recording system on the recording track of a magneto-optic disk 1, and is obtained by tracing the recording track of a magneto-optic disk 1 by the laser beam by the optical head 53 — the RF circuit 55 — binary — it has the decoder 71-izing [the decoder] and supplied. Not only this Tokimitsu magnetic disk but the readout of the same optical disk only for playbacks as the so-called CD (compact disk: Compact Disc) can be performed.

[0053] Corresponding to the encoder 65 in an above-mentioned recording system, about the playback output made binary by the RF circuit 55, a decoder 71 processes decryption processing, EFM decryption processing, etc. like **** for an error correction, and reproduces the ATC audio data of the above-mentioned data compression rates 1/8 with the transfer rate of 75 sectors / second earlier than the transfer rate of normal. The playback data obtained by this decoder 71 are supplied to memory 72.

[0054] Writing and read-out of data are controlled by the system controller 57, and memory (RAM) 72 is written in at the transfer rate of 75 sectors / second of those burstily [the playback data supplied with the transfer rate of 75 sectors / second from a decoder 71]. Moreover, this memory 72 is continuously read with the transfer rate of the 9.375 sectors / second corresponding to data compression rates 1/8 in the above-mentioned playback data burstily written in with the transfer rate of the above-mentioned 75 sectors / second.

[0055] A system controller 57 performs memory control which reads the above-mentioned playback data from memory 72 continuously with the transfer rate of the above-mentioned 9.375 sectors / second while writing playback data in memory 72 with the transfer rate of 75 sectors / second. Moreover, a system controller 57 controls a playback location to reproduce continuously the above-mentioned playback data burstily written in by this memory control from memory 72 from the recording track of a magneto-optic disk 1 while performing memory control like **** to memory 72. Control of this playback location manages the playback location of the above-mentioned playback data burstily read from memory 72 by the system controller 57, and is performed by supplying the control signal which specifies the playback location on the recording track of a magneto-optic disk 1 or an optical disk 1 to the servo control circuit 56.

[0056] The ATC audio data obtained as playback data continuously read from memory 72 with the transfer rate of 9.375 sectors / second are supplied to the ATC decoder 73. This ATC decoder 73 corresponds to the ATC encoder 63 of the above-mentioned recording system, and 16-bit digital audio data are reproduced by increasing data elongation (bit elongation) of the ATC data 8 times. The digital audio data from this ATC decoder 73 are supplied to D/A converter 74.

[0057] D/A converter 74 changes into an analog signal the digital audio data supplied from the ATC decoder 73, and is the analog audio output signal Aout. It forms. Analog audio signal Aout obtained by this D/A converter 74 It is outputted from an output terminal 76 through a low pass filter 75.

[0058] Next, high efficiency compression coding is explained in full detail. That is, they are band division coding (SBC) and adaptive transform coding (ATC:Adaptive Transform Coding) about input digital signals, such as an audio PCM signal. And the technique which carries out high efficiency coding using each technique of adaptation bit allocation is explained, referring to drawing 5 or subsequent ones.

[0059] Drawing 5 is the block diagram showing the outline configuration of the coding equipment of the acoustic wave form signal with which the gestalt of operation concerning this invention is applied. In the gestalt of this operation, each component is encoded by the signal-component coding means 1102, the signal wave form 101 where it was inputted serves as a signal 103, after being changed into the signal 102 of a signal frequency component by the conversion means 1101, and the sign train 104 is generated by the sign train generation means 1103.

[0060] Drawing 6 is the example of the conversion means 1101 of drawing 5, and the signal divided into two bands with the band division filter is changed into the spectrum signal components 221 and 222 in each band, respectively by the order spectrum conversion means 1211 and 1212, such as MDCT (MODIFAIIDO discrete cosine transform). The signal 201 of drawing 6 is equivalent to the signal 101 of drawing 5, and each signals 221 and 222 of drawing 6 are equivalent to the signal 102 of drawing 5. With the conversion means of drawing 6, the bandwidth of signals 211 and 212 is one half of the bandwidth of a signal 201, and is thinned out by one half of signals 201. Of course as a conversion means, a large number may be considered besides this example, for example, an input signal may be directly changed into a spectrum signal by MDCT, and you may change not by MDCT but by DFT (discrete Fourier transform) and DCT (discrete cosine transform). Although it is also possible to divide a signal into a band component with the so-called band division filter, the approach of this invention is convenient when the approach of changing into a frequency component by the above-mentioned spectrum conversion from which many frequency components are obtained in the comparatively small amount of operations is taken.

[0061] Drawing 7 shows the example of the signal-component coding means 1102 of drawing 5, based on the quantization precision (signal 303) calculated by the quantization precision decision means 1302, it quantizes with the quantization means 1303, and each signal component (signal 301) is taken out as a signal 304, after normalization is performed for every predetermined band by the normalization means 1301 (signal 302). Although the signal 301 of drawing 7 is equivalent to the signal 102 of drawing 5 and the signal 304 of drawing 7 is equivalent to the signal 103 of drawing 5, in addition to the quantized signal component, normalization multiplier information and quantization precision information are also included in the signal 304 here.

[0062] Drawing 8 is the block diagram showing an example of the decryption equipment which outputs an acoustic signal from the sign train generated by the coding equipment shown in drawing 5. In the decryption equipment of this drawing 8, after the sign 402 of each signal component is extracted from the sign train 401 by the sign train decomposition means 1401 and each signal component 403 is restored by the signal-component decryption means 1402 from those signs 402, the acoustic wave form signal 404 is outputted by the inverse transformation means 1403.

[0063] Although drawing 9 is the example of the inverse transformation means 1403 of drawing 8, this is a thing corresponding to the example of the conversion means of drawing 6, and the signals 511 and 512 of each band obtained by the reverse spectrum conversion means 1501 and 1502 are compounded with the band composition filter 1511. Each signals 501 and 502 of drawing 9 are equivalent to the signal 403 of drawing 8, and the signal 521 of drawing 9 is equivalent to the signal 404 of drawing 8.

[0064] Drawing 10 is drawing for explaining the approach of coding performed conventionally in the coding equipment shown in drawing 5. In the example of this drawing 10, a spectrum signal is acquired by the conversion means of drawing 6, and drawing 10 changes level into dB and shows the absolute value of the spectrum of MDCT. The input signal is changed into 64 spectrum signals for every predetermined time amount block, it packs it into eight bands of [1] to [8] in drawing (this is hereafter called a coding unit), and normalization and quantization are performed. By making it change with the methods of distribution of a frequency component for every coding unit, efficient coding in acoustic sense which presses down degradation of tone quality to the minimum is possible for quantization precision.

[0065] It is possible to raise coding effectiveness further to the approach described above. For example, coding effectiveness can be raised by assigning comparatively short code length to what has frequency high among the quantized spectrum signals, and assigning comparatively long code length to what has low frequency. Moreover, since the amount of sub information, such as quantization precision information and normalization multiplier information, can be reduced relatively, and frequency resolution is gone up by taking the long conversion block length for example, and quantization precision can be controlled warmer on a frequency shaft, coding effectiveness can be raised.

[0066] Drawing 11 shows the gestalt of implementation of the format based on the conventional

technique for recording the signal encoded by the above approaches. In this example, all bands are divided into B bands in all, and it counts from a low-pass side, and is W (i) about the quantifying bit number of the band of No. i (however, $1 \leq i \leq B$). Each of bit string [of a spectrum multiplier] Q (i) by which the normalization multiplier of the band of No. i was given to the normalization of S (i) and a band and quantization of No. i is recorded in the sequence shown in drawing 11.

[0067] While the gestalt of operation of the first here of this invention does not encipher to some signal components which can check the contents of software and enabling it to try listening the contents also with a general playback means Only those who received the key by enciphering to the signal component which furthermore enables playback of the quality of loud sound, and recording a signal are the things to which it is made for playback of the worthy quality of loud sound to be attained. By the approach of the gestalt operation of the first of this invention, drawing 12 shows the example of the sign train in the case of encoding.

[0068] That is, in the gestalt of operation shown in this drawing 12, the inputted information signal was divided into the low-pass component as the first signal component of low quality which can grasp the contents, and the high-frequency component as the second signal component for high quality playback, and only the second signal component of the above was enciphered and it has encoded.

[0069] Q (C+1) corresponding to the high-frequency component of an input signal in differing from the sign train of drawing 11 in the sign train of this drawing 12 from — Q (B) up to (however, $1 < C < B$) — a sign train is the point which is enciphered by the pseudo-random bit string and recorded as a sign train from R (Q (C+1)) to R (Q (B)).

[0070] If it is going to reproduce this sign train with the decryption equipment of drawing 8 (C+1) Although the signal of a high region from watch to No. B is correctly unreplicable since [of the spectrum multiplier normalized and quantized] the train is enciphered separately, a signal low-pass [from No. 1 to No. C] can be decoded correctly. Since an audition person can grasp the contents of the software by reproducing a low-pass signal correctly in this way since almost all amount of information is generally concentrating on the low-pass signal in the case of an acoustic signal, it can judge whether a key required for the nature playback of loud sound should be purchased by this.

[0071] By the way, when the coding approach like drawing 12 is taken and it reproduces with the decryption equipment of drawing 8, an unpleasant noise will be in a high region side. Then, the gestalt of implementation of the more desirable coding approach of this invention with which such a fault is compensated is explained, referring to drawing 13.

[0072] the gestalt of operation of drawing 12 with the gestalt of operation of drawing 13 — setting — W (C+1) from — W (B) Into the part on which the signal was recorded The information which shows that 0-bit assignment is performed as W (B) from W (C+1) is recorded, and the signal of W (C+1) to W (B) is recorded on the backmost part of the signal of this block. Moreover, coding is made as what has the number of bits fewer than the example of drawing 12 which the bit string of a spectrum multiplier to which a part required in order to record the signal of this W (C+1) to W (B), normalization, and quantization were performed uses.

[0073] Namely, it sets in the gestalt of operation shown in this drawing 13. While dividing the inputted information signal into the low-pass component of low quality which can grasp the contents, and the high-frequency component for high quality playback, enciphering only the above-mentioned high-frequency component and encoding as a sign train from R (Q (C+1)) to R (Q (B)) the information about this high-frequency component, for example, quantifying bit number information, — W for low quality playback (C+1) to W (B) up to — it has encoded at the duplex in the first sign train and the second sign train from W for high quality playback (C+1) to W (B).

[0074] When the bit string shown in this drawing 13 is reproduced with the decryption equipment of drawing 8, this decryption equipment (C+1) from — it being judged as that by which the bit is not assigned to the band to B, and, since the sign train from R (Q (C+1)) to R (Q (B)) is reproduced as what is not An unpleasant noise which was generated in the case of the example of drawing 12 is not generated, but the narrow output sound of a band is merely

reproduced. Thereby, although an audition person causes an unpleasant thought and does not have an end, if quality, it can judge whether it should try listening the sound which is not and this key should come to hand.

[0075] The signal which drawing 14 is what showed the example of the coding means for realizing the coding approach of the gestalt operation of drawing 13, and was encoded for every time amount block in this example using N bit shall be recorded on a record medium. [0076] In the gestalt of operation shown in this drawing 14, the inputted PCM signal 601 is changed into the signal 602 of a signal frequency component by the conversion means 1601. Next, like the coding equipment of drawing 5, for every predetermined band, normalization and quantization are performed and this signal 602 is encoded by the signal-component coding means 1602. Here, it sets to the coding equipment of drawing 5, and is M1 to coding of each quantifying bit number. It is M2 to coding of a bit and each normalization multiplier. To the bit string of a spectrum multiplier to which normalization and quantization were performed for every time amount block noting that the bit was used ($N - (M1 + M2) * B$) Bit assignment is performed as what can use a bit. On the other hand, it sets for the coding means of drawing 14. To the bit string of a spectrum multiplier to which normalization and quantization were performed for every time amount block ($N - (M1 + M2) * B - (B - C) * M1$) Bit assignment is performed as what can use a bit. The result is outputted as a signal 603 as Q (B) from S (B) from W (B) from W (1), and S (1), and Q (1).

[0077] Moreover, the exclusive OR of the pseudo-random bit string 606 which the pseudo-random bit string generating means 1604 outputted by making into initial value the key signal 605 which a control means 1603 generates, and the signal 603 which the signal-component coding means 1602 outputted is taken by the exclusive-OR means 1605, and the result is outputted as a signal 607. The sign train generation means 1606 combines alternatively the information on each signals 603 and 607, and zero signal equivalent to W' (B) from W' (C+1), and outputs the sign train 608 shown in drawing 13.

[0078] Drawing 15 shows the example of the decryption equipment for carrying out nature playback of loud sound of the sign train generated by the coding equipment of the configuration of drawing 14 as a gestalt of operation of this invention. In this drawing 15, from the sign train 901 of the format shown in drawing 13, the sign train decomposition means 1901 extracts Q (C) from S (B) from W (B) from W (1), and S (1), and Q (1), and R (Q (C+1)) to R (Q (B)), and is sent to the selection means 1905 and the exclusive-OR means 1902. On the other hand, by making into initial value the key signal 904 sent through the control means 1903, the pseudo-random bit string generating means 1904 generates the same pseudo-random bit string 905 as the signal 606 of drawing 14, and sends it to the exclusive-OR means 1902. The exclusive-OR means 1902 takes an exclusive OR with each signals 902 and 905, and sends the signal 906 which it is as a result to the selection means 1905.

[0079] With the selection means 1905, among [R] signals 902 (Q (C+1)), R (Q (B)) is transposed to Q (B) from Q (C+1) contained in a signal 906, and the signal 907 which it is as a result is sent to the signal-component coding means 1906 from from.

[0080] Although the above is processing when the key signal comes to hand, when the key signal does not come to hand, the selection means 1905 disregards R (Q (C+1)) to R (Q (B)) among signals 902, and sends zero signal to the signal-component coding means 1906 instead. By the signal-component coding means 1906 and the inverse transformation means 1907, like the decryption means of drawing 8, the PCM signal 909 is generated and the rest is outputted.

[0081] When taking the above-mentioned approach so that clearly also from the above explanation and it reproduces with the usual decode means of drawing 8, Or when it reproduces with the decode means of drawing 15, without a key coming to hand, since a noise does not occur, it is not unpleasant, but when [with a narrow playback band] playback is made comparatively qualitatively of bass, a key comes to hand and it reproduces with the decode means of drawing 15, the large nature playback of loud sound of a playback band is made.

[0082] It does not pass over the coding approach of drawing 13 in the gestalt of 1 operation of this invention. In addition, like drawing 16 Instead of enciphering from Q (C+1) to Q (B), the same effectiveness as the case where it encodes by the approach of drawing 13 is acquired also by enciphering W (C+1) to W (B), and making R (W (B)) from R (W (C+1)).

[0083] Drawing 17 is a flow chart which shows the example of the flow of the processing for encoding by the approach of drawing 16, and is processing of step S101 to the step S103. After calculating the information on W (B) from S (B) from S (1), and W (1), and Q (1) to Q (B), In step S104, W (C+1) to W (B) is enciphered, R (W (C+1)) to R (W (B)) is made, and the sign train of drawing 16 is generated combining these by processing of step S105 to the step S109.

[0084] On the other hand, drawing 18 shows the example of the flow of the processing for generating the signal component of the band which should be reproduced from the sign train of drawing 16. First, in step S201, number-of-bits information [by the side of low-pass] W (1) to W (C) is decrypted, next the normalization multiplier of all bands and S (1) to S (B) is decrypted in step S202, and the spectrum multiplier which is further set to step S203 and by which the low-pass side was normalized and quantized, and Q (1) to Q (C) is decrypted. Next, it divides, when a key is acquisition ending in step S204, and when that is not right, and if a key is acquisition ending, processing will move to step S205. At step S205, decrypt R (W (B)) using a key from the number-of-bits information R by the side of a high region (W (C+1)), and it sets to step S206 further. Then, the information on Q (C+1) to Q (B) is decrypted using W (C+1) to obtained W (B), and the signal component of No. 1 to No. B is generated at step S207 using the information acquired by the above. On the other hand, when a key is not acquisition ending, in step S208, only the signal component by the side of low-pass [of No. 1 to No. C] is generated.

[0085] As mentioned above, although the gestalt of another operation encoded based on the approach of this invention was described Various practices of this invention are considered. In addition, when the normalization multiplier of a very small value can be encoded Even if the decryption means of drawing 8 records the normalization multiplier value of a very small value on the location judged [having recorded the normalization multiplier by the side of a high region, and] and it records the true normalization multiplier apart from it instead of setting bit quota information to 0 There is almost no noise, and when it reproduces with the usual decode means of drawing 8 , or when it reproduces without a key coming to hand, although it is not unpleasant, playback of the quality of bass is made comparatively, and when [with a narrow playback band] a key comes to hand and it reproduces, on the other hand, the effectiveness that playback is made qualitatively of loud sound is acquired.

[0086] When similarly the encoded number of bands is also being recorded, the decryption means of drawing 8 records the information showing a narrow band on the location judged [having recorded the information and], and you may make it record the true number information of bands on it otherwise. Although it enables it to perform high quality playback, and various the approaches of enabling it to reproduce a part of signal are considered when that is not right only when a part of information on a sign is recorded on multiplex and one signal is used including these, these are all contained in the approach of this invention.

[0087] Moreover, although how to divide a signal into frequency shaft orientations and encipher the part above was described, it is also possible to divide a signal in the level direction and to encipher the part, and drawing 19 and drawing 20 show the gestalt of operation of the coding means for it, and a decryption means, respectively.

[0088] That is, in drawing 19 , the input PCM signal 753 is divided into the bit 754 by the side of low order, and the bit 755 by the side of a high order by the signal division means 1753, and only the bit 754 by the side of low order is again compounded with a high order bit by the signal composition means 1755, after a scramble is applied by the exclusive-OR means 1754. On the other hand, in drawing 20 , the same bit string 774 as the output 757 of the coding means of drawing 19 is divided into the bit 775 by the side of low order, and the bit 776 by the side of a high order, only the bit 775 by the side of low order is again compounded with a high order bit by the signal composition means 1775, after a scramble is canceled by the exclusive-OR means 1774, and the same PCM signal 778 as the input PCM signal 753 of drawing 19 is acquired.

[0089] However, when the direction which divided the signal in the frequency direction tries listening in the condition that the scramble is not solved, there is little sense of incongruity, without the ability hearing a noise. Moreover, since the information on the bit by the side of low order disappears in many cases in applying bit reduction, it is applicable to an application with wide range dividing a signal to the frequency direction.

[0090] As mentioned above, although explained taking the case of the case where an audio signal is used, the approach of this invention can be applied also to a picture signal. However, in the case of an audio signal, it is possible it to be effective to perform bit allocation accommodative especially because of tone-quality maintenance, and for the approach of recording the bit allocation information for it to be widely used by the band, and to apply the approach of this invention easily and effectively by it.

[0091] Moreover, although the approach enciphered using the key information corresponding to each music was described above, it is also possible for the approach of this invention to encode information required for the nature playback of loud sound with a secret common algorithm possible [applying, even if it is not necessarily the case where the key information corresponding to each music is used]. In this case, the specification for the nature playback of loud sound itself is a kind of key, and such a case is included with the encryption in description of this invention. however, it cannot be overemphasized by managing using key information actually boiling every music or medium that safer distribution-of-information processing is possible.

[0092] Moreover, although the case where the encoded bit stream was recorded on a record medium above was explained Also when transmitting a bit stream, can apply the approach of this invention, and by this, although only the listener who received the key can be made to do nature playback of loud sound and the contents can grasp enough the audio signal currently broadcast to other listeners, for example Only playback by the quality of bass is able to be able to be made to perform comparatively.

[0093]

[Effect of the Invention] The first signal component of quality with low extent which can grasp the contents for the inputted information signal according to this invention so that clearly also from the above explanation, there is no key information on encryption by dividing into the second signal component for high quality playback, enciphering only the second signal component of the above and encoding — ** — quality with low extent which can grasp the contents by the first signal component can be reproduced, and high quality playback can be performed by using key information.

[0094] Therefore, after checking the contents of software, it became possible to judge whether key information required for high quality playback should come to hand, and it became possible to distribute smoother software. Furthermore, although it is the quality of bass comparatively even if it uses a regenerative apparatus without the function of code discharge by this invention Since the contents of the music etc. can be known, become possible to try listening using the usual regenerative apparatus during commutation, and more candidates are received, for example. It became possible to make the audition for making a judgment of whether the music of the same contents as it should purchase the disk currently recorded qualitatively of loud sound perform. Furthermore, by the approach of this invention, also when performing high efficiency coding, the encryption which achieves the above-mentioned purpose is attained.

[0095] Moreover, the first sign of the above can perform playback of low quality by encoding to a duplex at the first sign for low quality playback, and the second sign for high quality playback about a part of information, for example, the information about the second signal component of the above, without receiving bad influences, such as a noise by the second signal component of the above, by reproducing by not enciphering using this first sign. This enables playback of comparatively the low quality in the regenerative apparatus of the large range, when the sign train which was encoded and was acquired makes it the sign train which is meaningful also for a playback means without a key.

[Translation done.]

* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram showing an example of the configuration for enciphering an information signal.

[Drawing 2] It is the block diagram showing an example of the configuration for decrypting the sign train which enciphered the information signal.

[Drawing 3] It is drawing for explaining one approach for enciphering and decrypting.

[Drawing 4] It is the block circuit diagram showing the outline configuration of an example of the compressed data record and/or the regenerative apparatus with which the gestalt of operation of this invention is applied.

[Drawing 5] It is the block diagram showing an example of the coding equipment with which explanation of this invention is presented.

[Drawing 6] It is the block diagram showing the example of the conversion means of the coding equipment of drawing 5.

[Drawing 7] It is the block diagram showing the example of the signal-component coding means of the coding equipment of drawing 5.

[Drawing 8] It is the block diagram showing the example of the decryption equipment with which explanation of this invention is presented.

[Drawing 9] It is the block diagram showing the example of the inverse transformation means of the decryption equipment of drawing 8.

[Drawing 10] It is drawing for explaining the coding approach with which explanation of this invention is presented.

[Drawing 11] It is drawing for explaining an example of the sign train acquired by the coding approach with which explanation of this invention is presented.

[Drawing 12] It is drawing for explaining an example of the sign train acquired according to the gestalt of operation of this invention **** coding approach.

[Drawing 13] It is drawing for explaining an example of the sign train acquired according to the gestalt of other operations of this invention **** coding approach.

[Drawing 14] It is the block diagram showing an example of the coding equipment with which the gestalt of operation concerning this invention was applied.

[Drawing 15] It is the block diagram showing the gestalt of operation of the decryption equipment concerning this invention.

[Drawing 16] It is drawing for explaining an example of the sign train acquired according to the modification of the gestalt of other operations of this invention **** coding approach.

[Drawing 17] It is a flow chart for explaining an example of the coding approach for acquiring the sign train of drawing 16.

[Drawing 18] It is a flow chart for explaining an example of the decryption approach which decrypts the sign train of drawing 16. It is the flow chart showing the example of the decryption approach by this invention.

[Drawing 19] It is the block diagram showing the coding equipment with which the gestalt of other operations was applied to the pan concerning this invention.

[Drawing 20] It is the block diagram showing an example of the decryption equipment used as the gestalt of other operations in the pan concerning this invention.

[Description of Notations]

1601 Conversion Means, 1906 Signal-Component Decryption Means, 1907 Inverse-
Transformation Means 1602 Signal-Component Coding Means 1603, 1903, 1751, 1771 Control
Means 1604, 1904, 1752, 1772 Pseudo-random Bit String Generating Means 1605, 1902, 1754,
1774 Exclusive-OR Means 1601 Sign Train Generation Means 1901 Sign Train Decomposition
Means 1905 Selection Means

[Translation done.]

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

FADED TEXT OR DRAWING

BLURRED OR ILLEGIBLE TEXT OR DRAWING

SKEWED/SLANTED IMAGES

COLOR OR BLACK AND WHITE PHOTOGRAPHS

GRAY SCALE DOCUMENTS

LINES OR MARKS ON ORIGINAL DOCUMENT

REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.